18

EXPORT CONTROLS ON MASS MARKET SOFTWARE

Y 4.F 76/1:EX 7/32

Export Controls on Mass Market Soft...

HEARING

BEFORE THE

SUBCOMMITTEE ON
ECONOMIC POLICY, TRADE AND ENVIRONMENT

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

FIRST SESSION

OCTOBER 12, 1993

Printed for the use of the Committee on Foreign Affairs

SUPERINTENDENT OF DOCUMENTS
DEPOSITORY

MAR 16 1994

BOSTON PUBLIC LIBRARY
GOVERNMENT DOCUMENTS DEPARTMENT

U.S. GOVERNMENT PRINTING OFFICE
74-648 CC
WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-043370-3

18

EXPORT CONTROLS ON MASS MARKET SOFTWARE

Y 4. F 76/1: EX 7/32

Export Controls on Mass Market Soft...

HEARING

BEFORE THE

SUBCOMMITTEE ON
ECONOMIC POLICY, TRADE AND ENVIRONMENT

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRD CONGRESS

FIRST SESSION

OCTOBER 12, 1993

Printed for the use of the Committee on Foreign Affairs

SUPERINTENDENT OF DOCUMENTS
DEPOSITORY

MAR 16 1994

BOSTON PUBLIC LIBRARY
GOVERNMENT DOCUMENTS DEPARTMENT

U.S. GOVERNMENT PRINTING OFFICE
74–648 CC WASHINGTON : 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-043370-3

COMMITTEE ON FOREIGN AFFAIRS

LEE H. HAMILTON, Indiana, *Chairman*

SAM GEJDENSON, Connecticut
TOM LANTOS, California
ROBERT G. TORRICELLI, New Jersey
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
HARRY JOHNSTON, Florida
ELIOT L. ENGEL, New York
ENI F.H. FALEOMAVAEGA, American Samoa
JAMES L. OBERSTAR, Minnesota
CHARLES E. SCHUMER, New York
MATTHEW G. MARTINEZ, California
ROBERT A. BORSKI, Pennsylvania
DONALD M. PAYNE, New Jersey
ROBERT E. ANDREWS, New Jersey
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
CYNTHIA A. McKINNEY, Georgia
MARIA CANTWELL, Washington
ALCEE L. HASTINGS, Florida
ERIC FINGERHUT, Ohio
PETER DEUTSCH, Florida
ALBERT RUSSELL WYNN, Maryland
DON EDWARDS, California
FRANK McCLOSKEY, Indiana
THOMAS C. SAWYER, Ohio
(Vacancy)

BENJAMIN A. GILMAN, New York
WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
TOBY ROTH, Wisconsin
OLYMPIA J. SNOWE, Maine
HENRY J. HYDE, Illinois
DOUG BEREUTER, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
JAN MEYERS, Kansas
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California
DAVID A. LEVY, New York
DONALD A. MANZULLO, Illinois
LINCOLN DIAZ-BALART, Florida
EDWARD R. ROYCE, California

Michael H. Van Dusen, *Chief of Staff*
Richard J. Garon, *Minority Chief of Staff*
Anne Grey, *Staff Associate*

Subcommittee on Economic Policy, Trade and Environment

SAM GEJDENSON, Connecticut, *Chairman*

JAMES L. OBERSTAR, Minnesota
CYNTHIA A. McKINNEY, Georgia
MARIA CANTWELL, Washington
ERIC FINGERHUT, Ohio
ALBERT RUSSELL WYNN, Maryland
HARRY JOHNSTON, Florida
ELIOT L. ENGEL, New York
CHARLES E. SCHUMER, New York

TOBY ROTH, Wisconsin
DONALD A. MANZULLO, Illinois
DOUG BEREUTER, Nebraska
JAN MEYERS, Kansas
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California

John Scheibel, *Staff Director*
Edmund B. Rice, *Republican Professional Staff Member*
Kathleen Bertelsen, *Professional Staff Member*
Donna La Torre, *Professional Staff Member*
Peter Yeo, *Professional Staff Member*

CONTENTS

Page

WITNESSES

James Hendren, president, Arkansas Systems 3
Raymond Ozzie, president, IRIS Associates, representing the Business Software Association 5
Steven T. Walker, president, Trusted Information System, Inc. 10
Philip Zimmerman, Cryptograph Consultant 20
Don Harbert, vice president, software engineering, Digital Equipment Corporation 23

APPENDIX

Prepared statements:
- Hon. Sam Gejdenson 31
- James Hendren 31
- Raymond Ozzie 33
- Steven T. Walker 48
- Philip Zimmerman 105
- Don Harbert 111

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Frost & Sullivan Report, "The Demand for Information Security and Encryption in Fortune 500 Comapnies in the United States", prepared for Business Software Alliance 120
"Implications of Encryption Policy on the National Information Infrastructure", submitted by Business Software Alliance 125
"A Primer on Telephone Surveillance for Human Rights Organizations", by David Banisar, Washington Office, Privacy International 134

EXPORT CONTROLS ON MASS MARKET SOFTWARE

TUESDAY, OCTOBER 12, 1993

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FOREIGN AFFAIRS,
SUBCOMMITTEE ON ECONOMIC POLICY,
TRADE AND ENVIRONMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 1:30 p.m. in room 2172, Rayburn House Office Building, Hon. Sam Gejdenson (chairman of the subcommittee) presiding.

Mr. GEJDENSON. A number of members of the subcommittee, including Mr. Roth our ranking member, are involved in another Foreign Affairs Committee meeting and we hope they will be able to join us later. We appreciate all of the assistance, particularly from Mr. Roth and his crack staff for the job they have done through the years. And we understand the multiplicity of meetings that go on.

This hearing is about the well-intentioned attempts of the National Security Agency to control that which is uncontrollable. The NSA seeks to restrict the export of software which is sold in the United States on a mass market basis.

You can go into a software store in virtually any mall in the United States and buy this software. The NSA itself acknowledges that if you have a long-distance telephone line and a modem, you can send this software anywhere in the world. If you have a computer and a modem, you can take this software off the Internet anywhere in the world. But NSA seeks to control its sale not only to countries like Iran, but to countries like Taiwan, Singapore, and even to the United Kingdom and France.

Not only must we wonder why the United States seeks to limit our sales to our NATO allies and to others in the free world, but why does NSA think it is possible? The issue is not whether individuals in these markets will obtain such software. They certainly will. The issue is whether they will get it legally or illegally and whether they will get it from an American company or from a foreign company.

I do not question the value of the information sought by the National Security Agency. But once it is determined that the dispersion of this software cannot be controlled, then however much as we might want to protect our ability to obtain information, it is beyond our means to do so.

Just as in the case of telecommunications, the National Security Agency is attempting to put the genie back in the bottle. In my opinion, it won't happen. And a vibrant and productive sector of American industry may be sacrificed in the process.

Not but a month or two ago, we had AT&T here with pictures of a 565 switching station for telephones made by the Chinese; we had a 623 switching station made by the Israelis legally sold to the Chinese while the American Government was restricting AT&T's ability to sell the 565 switching station.

It merely creates competitiveness for American products, in my opinion. It gives opportunities for foreigners to enter the market that we now dominate, and we could see very well as the automobile industry once dominated America's automobile sales in much of the world, as we did in other industries, see this vibrant industry, as a result of our own government actions, be injured in the future.

Ms. Cantwell, an opening statement?

[The prepared statement of Mr. Gejdenson appears in the appendix.]

Ms. CANTWELL. Thank you, Mr. Chairman. And I appreciate your great efforts in bringing this hearing before us today.

We are here to discuss, really, competing visions of the future. One is really a reflection of the speed and dexterity of the new information age facing us and the ability of our Nation's software manufacturers to compete in a global economy. The other is constrained by those with legitimate concerns, by those who are willing to shoulder the inevitable at the expense of a dynamic American industry.

In recent months, both the President and Vice President have spent considerable time explaining their vision of a national information infrastructure that is essential to our future economic growth. Driving that vision is personal computers, and at the heart of every computer is computer software.

Just 2 weeks ago the Clinton administration, recognizing the importance of updating our export control policies, announced its intentions to relax controls on computers and telecommunication equipment. I applaud these efforts and commend the administration for the beginning of a process of examining our export control policies.

Clearly, the decision resulting in relaxing these controls recognizes the economic reality of outdated controls. But nowhere in that announcement were the concerns of the software industry. The time has come for us to address the export controls on generally available software, including software with encryption technology. This is not a new issue. In the last Congress, the House of Representatives passed legislation by a sizable margin that would have relaxed the control on mass market software, including software with encryption technology.

At issue today is our Government control of the export of generally available software with encryption or information security capabilities, the very same sling wrap software that is available for anyone who walks in to Egghead or Computerland software stores.

Our Government unilaterally controls the sales of software with encryption capabilities. Our allies don't control it. In fact, CoCom moved to decontrol it 2½ years ago. In fact, there are hundreds of foreign encryption programs currently being sold throughout the world. In addition, anyone with a modem or telephone can download it from just about anywhere in the world.

Clearly, we must ensure that one of the fastest growing American industries, one that accounts for $36—over $36 billion in value added to the U.S. economy in 1992, is not placed at a competitive disadvantage because of our export control policies. In fact, a recent estimate shows that the industry stands to lose between $6 and $9 billion annually if we don't act.

What we are debating today is not just an academic exercise. Our actions in this Congress means future sales, markets, and high skills and high wage jobs. We would rather see policy considerations given or legislation, if needed, to resolve this issue. This issue is simply too important for the future success of what is a vital U.S. industry.

I look forward to the testimony today and look forward to working with Chairman Gejdenson on this issue and the leadership of the ranking minority member as well to resolve this very important problem.

Thank you, Mr. Chairman.

Mr. GEJDENSON. The gentleman from Ohio.

Mr. FINGERHUT. Thank you, Mr. Chairman.

I just want to reiterate comments I have made at previous hearings of this subcommittee, and that is that I believe that this subcommittee has its finger on an issue which is central to the question of how to unlock the potential of this economy and promote economic growth.

While in places all over this city people are debating the subject of economic growth, this subcommittee recognizes that the progress that can be made in our economy will be made through increasing exports and that we have been hamstringing ourselves in the process of making this trade grow.

This is an important subject today in dealing with the subject of software. It adds to the other efforts that you, Mr. Chairman of this subcommittee, have made in this area. I hope that we can move quickly to pass relevant legislation to lift these export controls and to allow both these gentlemen who sit here and the companies all over the country, in Ms. Cantwell's district and in mine, to begin to compete in the world marketplace immediately.

Thank you.

Mr. GEJDENSON. Thank you.

The witnesses on our first panel are Dr. James Hendren, president, Arkansas Systems; Raymond Ozzie, president, IRIS Associates, representing the Business Software Association; Steven T. Walker, president, Trusted Information Systems, Inc.; Philip Zimmerman, cryptograph consultant, and Don Harbert, vice president, Software Engineering, Digital Equipment Corporation.

Doctor, do you want to start?

STATEMENT OF JAMES HENDREN, PRESIDENT, ARKANSAS SYSTEMS

Mr. HENDREN. Thank you, Mr. Chairman.

Let me first give you a little background on Arkansas Systems and our relationship to the topic of export of encrypted software and hardware.

Arkansas Systems works primarily in the finance industry and concentrates on providing software to improve the effectiveness of payment systems worldwide. This includes the technologies related to automatic teller machines, national and international switching of payment transactions, check processing, and the remittance payments of commercially generated bills.

Arkansas Systems has customer installations in 39 countries, including Southeast Asia, Latin America, and Eastern Europe, including Russia.

Arkansas Systems is a 17-year-old company with about 100 employees, doing about $10 million in revenue per year and with about 40 percent of that revenue being international.

In the finance industry, the Data Encryption Standard, or DES, algorithm is an international standard for encrypting payment transactions such as ATM, automatic teller machine withdrawal transactions; and is, as you are aware, approved for delivery to selected other countries if it is delivered to a bank. This makes the algorithm readily available, both in software and in hardware devices.

The biggest problem that we have in using DES internationally is the significant, sometimes 4 to 6, weeks delay it takes to get shipment approved. This delays completing projects and adds additional cost to the project. It produces needless overhead costs associated with the export of both our products and the products of the hardware vendors with which we work. The approval has always been granted for every project with a financial institution in which we have been involved.

Right now, however, we have a project with the Central Bank of Russia which is very much delayed getting that approval; but it is a bank, and I am sure it will eventually be approved.

When we work with nondepository institutions such as a finance company and need to use the same industry——

Mr. GEJDENSON. How long have you been waiting for the Russia approval?

Mr. HENDREN. It has been a little over 6 weeks.

Mr. GEJDENSON. Six weeks. Thank you.

Mr. HENDREN. So when we work with nondepository institutions such as a finance company and we need to use the same industry standard processes, the approval is extremely difficult to get and sometimes not given at all.

Let me give you an example. We were working with an international oil company. They wanted to credit their employees' payroll accounts and let the employees withdraw funds as they needed them via a debit point of sale wherever in the world the employee might be. The roadblock that eventually stymied this project was the impossibility of being able to use the DES algorithm on the network due to export restrictions. International point of sale networks, run by institutions other than banks, are having to use nonstandard encryption equipment and, therefore, cannot interconnect to existing financial networks in accepted ways.

Now, let's discuss the DES algorithm in particular. The mathematical algorithm itself is readily available. We acquired copies of the algorithm from the dollar sale table at the local bookstore in

Little Rock, Arkansas, and from a published article in *Scientific American Magazine.*

Our business-oriented programming staff has written three different versions of this algorithm. Each was developed in a very short timeframe, and one of these has been certified by the National Bureau of Standards. Any user anywhere in the world could do this also. Trying to limit such a readily buildable product is rather ridiculous.

I would also like to relate some of our experiences in Russia working with the Russian banks. The security methods available to the commercial world in Russia are very sophisticated; and these bankers, in our experience, are much more security conscious than our U.S. counterparts. Our DES method works well, and most people are very happy with the way the security is handled in the United States. But we have had difficulty in trying to convince the Russians that DES is good enough. Some of our projects require certifying security plans for financial transactions with FAPSI, that is the Russian Federal Security Office.

What they look at is much more involved than just using DES. They want to look at RSA and FIAT SHAMIR algorithms and multiple layers of encryption, again, trying to restrict an old, proven technology that everyone is using and that our foreign former enemies consider inadequate is really a waste of effort.

In summary, we at Arkansas Systems believe that the export controls on software and hardware containing the DES algorithm is needless red tape that only impedes international commerce and does not preserve any advantage for the United States in any way. The trade association Information Technology Association of America, ITAA, of which we are members, also agrees with this position.

I would be happy to respond to your questions.

Mr. GEJDENSON. Thank you, sir.

[The prepared statement of Mr. Hendren appears in the appendix.]

Mr. GEJDENSON. Mr. Ozzie, are you next?

STATEMENT OF RAY OZZIE, PRESIDENT, IRIS ASSOCIATES, REPRESENTING THE BUSINESS SOFTWARE ASSOCIATION

Mr. OZZIE. Yes. Good afternoon.

I am Ray Ozzie, founder and president of IRIS Associates, a software development company.

Our principal product is work group application software marketed by Lotus Development Corporation.

Mr. GEJDENSON. Are you about to use the projector?

Mr. OZZIE. Yes, I am.

Mr. GEJDENSON. Maybe we should have the staff dim the lights there.

Mr. OZZIE. Thank you.

Mr. GEJDENSON. This is very impressive. Now, is this connected by a line to your computer?

Mr. OZZIE. Yes, sir. This telephone line right here goes from my computer out through your PBX to a system in Cambridge, Massachusetts, at MIT.

Mr. GEJDENSON. This is off of a central system in Cambridge, Massachusetts?

Mr. OZZIE. That is right.

I was going to demonstrate here, how easy it is to download DES implementations from anywhere in the world.

Right now I am connected live to the Internet, which I am sure that you are familiar with. Everything that I am showing you is commercially widely available. This laptop is widely available, as is Microsoft Windows, which is very easy to use, and 25 million copies have been sold. This program I am using is called FTP. It is File Transfer Program. It is intended for moving files from one part of the network to the other.

What I am going to do right now is connect to a system that I found last Friday. I spent 15 minutes looking for DES algorithms worldwide using a very simple search program that is available. Right now I am connecting into Germany. And as you can see on the screen——

Mr. GEJDENSON. You are dialing up Germany as we speak?

Mr. OZZIE. As we speak.

If you look at the bottom, it says "retrieving directly list." And here we are. We are now connected to NET, Europe, Germany, the program FTP on their side.

As you can see in this program, the screen is divided into two sides, one local, the other remote. This remote side is showing you what I am looking at in Germany, and the local side is showing you what I am looking at on my local computer.

If I type something over here called "pub utils," that is going into a directory on the remote computer in Germany where they store public utilities, things that might be of general utility to the public. And right now——

Mr. GEJDENSON. Not "public utilities" like electric companies, but files that have usability——

Mr. OZZIE. Files that might be of general usefulness.

Mr. GEJDENSON. So this isn't for any particular group of high tech guys?

Mr. OZZIE. No, it isn't. No. This is—unfortunately, it is taking a few minutes here.

Mr. GEJDENSON. That is all right.

Mr. OZZIE. The network tends to slow down during the day.

Let me tell you in advance what I am going to show you.

Last Friday, when I did the search, I tried to locate anything on the network that was DES. I found hundreds and hundreds of computers all over the world with DES. This particular computer I found interesting because it had two implementations of DES. If you look right here, there is one called "DES" and one called "DES-no-USA."

Mr. GEJDENSON. Why is it "no USA"?

Mr. OZZIE. I am going to show you. But essentially the one that is in the DES directory was implemented at Belcore. It was somehow retrieved out of the United States and put onto this computer system in Germany.

The "DES-no-USA" was written by someone in Finland. And it is essentially "clean" from their standpoint.

Mr. GEJDENSON. They don't trust our DES. Is that what you are saying?

Mr. OZZIE. No. I could show you—and it would be a little time consuming—that the foreign implementation is just as good.

Right now, let me just press this button. I am going to copy right now, and it is going to start copying.

Mr. GEJDENSON. How long will this take to copy?

Mr. OZZIE. This will take about 10 seconds. It is probably going to take a little longer than that right now.

Mr. GEJDENSON. OK.

Mr. OZZIE. One of the files that is inside this little package that I am downloading is documentation related to what I am downloading. And it specifically states that this algorithm, the source code for this, could be integrated into a product and it could be run against the National Bureau of Standards validation suite.

And as a matter of fact, they suggest that you run it against the U.S. Belcore implementation just to satisfy yourself that it is the full implementation.

Mr. GEJDENSON. So now you will hit "copy."

Mr. OZZIE. Yes, I did. It is basically done.

Mr. GEJDENSON. Oh, I see. The other day, I was not on the Internet, but I was picking up some math programs for my kid, and again, the same kind of thing. The programs ran everywhere from about, you know, a minute or two up to 18 minutes for the really long ones but not any particular skill.

Mr. OZZIE. That is right. This really is no particular skill. In the old days, it used to be very hard to use interface.

So that is it. Now we have it down.

Now I just want to show you one thing. On my screen, these buttons are about an inch apart. If I press this button right here, I would be exporting software.

Mr. GEJDENSON. Right.

Mr. OZZIE. OK. So I am not going to press that button.

Mr. GEJDENSON. Let me ask you this: You now have a DES software product in your file?

Mr. OZZIE. That is right.

Mr. GEJDENSON. And if you dialed me up in Iraq, and you were a bad guy, you would just hit that same copy button and send it to me?

Mr. OZZIE. What I would do is I would say disconnect here, and I'd say connect to the new one, and I would type in the name of your system. In this case I have—oh, here is one in Finland.

Mr. GEJDENSON. So would you be breaking the law.

Mr. OZZIE. Absolutely.

Mr. GEJDENSON. No, right now. Having just imported that from Germany, but it is a DES system, you can't export a DES system from the United States without a license; is that correct?

Mr. OZZIE. That is correct.

Mr. GEJDENSON. So if you were to now, a minute later, take this DES system and send it to somebody in England, you would be breaking the law?

Mr. OZZIE. That is right.

Mr. GEJDENSON. Even though you just brought it in from Germany?

Mr. OZZIE. That is correct.

Mr. GEJDENSON. So if you were to take a product that was worldwide available on this network to anybody in the globe and put it on the end of your Lotus product, even though it was not made in the United States, it was not developed in the United States, it is generally available worldwide, and package them together, you would be breaking the law?

Mr. OZZIE. Yes. The answer is yes.

And furthermore, even if I package my software with no cryptographic software, not one iota of cryptographic software, and instead put an open interface into it saying, if you get this software in Germany, plug in your own encryption, I could not export my software even though it had no cryptographic capability.

Mr. GEJDENSON. Now, on the other hand, if somebody was at home not familiar with all the export laws and they had your Lotus program in your computer and their friend was in Germany or Finland or anywhere else, they could, just as quickly, send your whole American Lotus program, including encryption, to Germany?

Mr. OZZIE. Yes.

Mr. GEJDENSON. They would be violating the law, of course; but they might not be aware of it.

Mr. OZZIE. They probably wouldn't be aware of it, but they would be violating the law.

Mr. GEJDENSON. And if they were intent on violating the law, they certainly could do it?

Mr. OZZIE. They certainly could do it. They could take a floppy disk and put it in their shirt pocket and get on an airplane. They could connect their modem to someone else and just transfer it that way.

The point here is that the cat is out of the bag. It is too late, and you can't get the cat back in. It is too easy. You know, cryptographic products and techniques are all over the world. Countries such as Israel and the former Soviet Union have produced world class cryptographers and mathematicians who are offering their skills on the open market. Regulations can stop U.S. products from reaching overseas markets, but they can't stop the free flow of knowledge.

Mr. GEJDENSON. And the folks in the National Security Agency will explain to us why, of course, this isn't a problem. Whether you leave—in a secret session, I am sorry to say.

Mr. OZZIE. Yes, I suppose they will. But it is a problem that is truly hurting the U.S. software industry. It is hurting it in an increasing fashion because people are asking more and more for software products that contain encryption.

The Business Software Alliance commissioned a survey of companies to review the demand for data encryption, and it found that 90 percent of the companies surveyed said that security is important; 46 percent specifically said that data encryption is important; and that 37 percent said that they specifically looked for encryption capabilities in the software that they purchase and would consider purchasing foreign software with otherwise less desirable features if it had security. That represents about $6 to $9 billion of revenues to American software companies that are at risk.

Mr. GEJDENSON. Let me just—I hate to keep interrupting, and I will give up my 5 minutes at the beginning so that I don't take advantage of my colleagues.

But just on this point, some folks would argue with that saying that, well, if you poll people and you ask them if they won a Rolls Royce and a Ferrari, they will check those off first. But if you tell them that what they can get is a Chevrolet or a Corvette, they will settle for those. So that some people would argue that your statement, while accurate, indicates that people, given their druthers, would like to have DES or triple DES and that would be all very nice; but if that is not available, then they will buy from you what you presently have available.

Mr. OZZIE. OK, let me speak to that issue.

I do presently have available this product, Lotus Notes, both in the United States and overseas. If you can see this box, it has a big "NFE," "Not For Export," label on it. That is because this is a North American edition with strong encryption. We can export this freely to Canada and sell it in the United States, but that is it. Overseas, we do sell a product that the NSA has approved for export and it has 40-bit encryption. NSA says this is good encryption; but let's just talk to the buyers.

Normally BSA members, including Lotus, earn approximately 50 to 55 percent of their revenue from overseas sales; the rest is here in the United States. For Lotus Notes, the number is more like 25 to 30 percent overseas. Why? Because the customers perceive the product not to be secure. They come to us telling us, we want DES, we want triple DES, we want 64-bit RC2. They come to us as educated customers and tell us what they want, and this is slowing us down tremendously. We are, indeed, losing sales.

So you know, this is beyond merely a survey.

Mr. GEJDENSON. Do you need the screen any more?

Mr. OZZIE. No, I really don't.

Mr. GEJDENSON. OK. Very impressive.

Now, the product on top which is not yours can hook to any computer that is made for overhead projectors?

Mr. OZZIE. Absolutely, yes.

Mr. GEJDENSON. Thank you.

Does the staff want to put the lights back on. And maybe you want to shut that—that is from a liquid crystal screen from a location—the computer is in Massachusetts?

Mr. OZZIE. Actually, it is this computer talking directly to the network—to the computer in Germany. Everything that is in between is just simply network. There is no real computer that I am specifically talking to.

Mr. GEJDENSON. Does somebody want to turn the lights back on and kill the overhead projector.

Go ahead.

Mr. OZZIE. Anyway, 9 years ago, I had the vision to do this product. It is an information management product, and customers really want it now. Some of the hottest selling software right now is to manipulate information back and forth.

Now, 9 years later, I have another vision of the future, actually two visions.

In the first one, the current export regulations will stay intact and we in the United States will keep on shipping products with the NFE export label. At the same time, enterprising foreign software producers will take advantage of our weakness and gain a foothold on their own turf. By the time we realize the magnitude of our mistake, we will have lost our advantage to these local producers. Again, I want to emphasize, today we are risking revenues of between $6 and $9 billion out of total revenues of between $18 and $27 billion.

In my second vision I see us putting a different label on software products, "Made in the USA" label, and we sell our programs with encryption overseas just like we sell other programs overseas right now. By doing this, we will be able to retain the current 75 percent market share worldwide that we currently enjoy on the other types of products. But if we don't relax the export controls, we are going to lose market share in this type of product overseas.

I would really like that second vision to come true, but we can't do it with the current unrealistic unilateral U.S. munitions export controls.

As many well-meaning people point out to you, the spread of strong encryption does, indeed, make the techniques of foreign intelligence gathering significantly more difficult. We don't dispute this fact. But the cat is out of the bag, and we can't put it back. Any criminal, foreign army or corporation or man on the street can gain access to cryptology here today.

My colleagues will shortly tell you about a recent study by the SPA regarding the number of high quality encryption programs on the market, and I just showed you what could be done with programs in the public domain.

I just want to reiterate, in closing, regulations can stop U.S. products from reaching overseas market; but they can't stop the free flow of knowledge. Consider the encryption technology that is taught in computer science courses around the world, and it is a subject of dedicated periodicals, and it is discussed at international conferences.

As you said, consider that any program that is sold in the United States, such as Lotus with DES, in fact, does become available abroad because all it takes is a floppy disk in a shirt pocket or a computer with a modem to communicate it overseas.

Generally available PC software is just that, generally available. American software companies must be permitted to sell worldwide DES or other equivalent strength algorithms in an unrestricted manner. We have enough trouble competing with the global marketplace. Export laws should not make it even more difficult.

Thank you.

Mr. GEJDENSON. Thank you.

[The prepared statement of Mr. Ozzie appears in the appendix.]

Mr. GEJDENSON. Mr. Walker.

STATEMENT OF STEVE WALKER, PRESIDENT, TRUSTED INFORMATION SYSTEMS, INC.

Mr. WALKER. Thank you.

My name is Steve Walker, founder and president of Trusted Information Systems, a 10-year-old small business with offices throughout the United States and in England, specializing in research, product development, and consulting and information security.

I am also here representing the Software Publishers Association and its members on this most important topic.

My background includes 22 years with the Department of Defense, at the National Security Agency, the Defense Advanced Research Projects Agency, and the Office of the Secretary of Defense.

My last job with the government was as Director of Information Systems for the Assistant Secretary of Defense for Communications, Command, Control and Intelligence. I have been a member of the Computer System Security and Privacy Advisory Board chartered by the Computer Security Act of 1987 throughout its many deliberations on cryptography.

My written testimony describes the national dilemma that has already been referred to here between, on the one hand, the interests of law enforcement and the national security to limit the availability of good quality cryptography so that they can continue to listen to our adversaries and, on the other hand, the rapidly growing interests worldwide of individuals and businesses to protect their sensitive information.

The tension between these forces has been building for years and is reaching a crisis stage. But the arguments on both sides have been mostly gloomy predictions of disaster. From the government, disaster if we open exports of cryptography; and from industry, disaster if we don't.

I am very pleased, therefore, to be here today to present some concrete evidence that may begin to move this debate from a war of words to a careful analysis of factual information that is so badly needed.

In May of this year, the Software Publishers Association chartered a survey of the worldwide availability of good quality cryptography. The findings to date indicate that cryptography is available now to essentially anyone who wants it.

This chart gives the findings as of today. Within just 5 months of part-time effort on the part of a few dedicated people, we have confirmed product literature and, in a few cases, actual software for 200 foreign products, 123 of which use the Data Encryption Standard algorithm, the official United States and de facto worldwide encryption standard.

We have leads that we are confirming on another 64 foreign products, giving a total of 264 products developed and available using cryptography outside the United States.

We have found manufacturers of cryptographic products in 21 foreign countries and distributors of cryptographic products in 33 countries worldwide.

Each orange dot represents a country in which there are one or more companies that are distributing or manufacturing cryptographic products right now, most of which is DES.

Most of the major countries in the Western Hemisphere are represented on this chart.

In the course of our survey, we have also confirmed the availability of 241 cryptographic products within the United States, 142 using DES; and we are attempting to confirm at least 47 others.

Worldwide, we have identified 552 products overall. The names and countries of origin of each of these products is in attachment 1 of my testimony.

We are continuing to find more products, manufacturers, and distributors on a daily basis. And we found five more companies yesterday, but we had closed off the database and we will report them next time.

We believe that we have just scratched the surface. We have assembled, over on my left, a set of notebooks which contain the product descriptions of all confirmed products in our databases. There are six that are U.S. domestic, and there are five, several of them quite tightly squeezed, that are foreign products. These are the products that are represented from the countries that are listed over here.

We have some of the sources of information that we have used to find these products. And, in addition, we have several of the products that we have purchased to confirm that good quality cryptography is, indeed, available worldwide.

There are a number of arguments that are frequently heard from those who wish to justify continued export controls. The first one frequently is, cryptographic products are not available outside the United States, so U.S. software and hardware developers are not hurt by export controls. We believe that the results of our survey thus far have proven that statement to be patently false.

A second argument is, even if cryptographic products are available, they cannot be purchased worldwide. Again our survey results, we believe, show this to be patently false. We have found 366 companies in 32 foreign countries and the United States that are manufacturing, marketing, and/or distributing cryptographic products, most on a worldwide basis. The names of these companies are listed in attachment 2 of my testimony.

A third argument that is frequently heard is even if the products are available and can be purchased easily, those sold in other parts of the world are somehow inferior to the products available in the United States.

To the contrary. The results of our survey again show that foreign products are just as good and, in many cases, better than many U.S. products. We have purchased products from several sources throughout the world.

We ordered DES-based PC file encryption programs for shipment to the U.S. from Algorithmic Research Limited in Israel; from Sophos, Limited in the United Kingdom; from Cryptomathic in Denmark; from CE Infosystems in Germany; and from uti-maco, also in Germany.

We have also obtained a similar product from Elias Limited, in Moscow, Russia, distributed through the EngRus Software International in the U.K. This product uses GOST, the Russian equivalent of DES.

All of the products we ordered were shipped to us in the United States within a few days. The German products were sent to us directly from their U.S. distributors in Virginia and Connecticut.

Our experience has been that if there was any export approval paperwork required by the governments of these companies, it is minimal and results essentially in immediate approval of shipping to friendly nations.

I will have more to say about that in a minute.

Mr. GEJDENSON. Can I just interrupt you a second?

Mr. WALKER. Certainly.

Mr. GEJDENSON. You are confident that every one of these products is as good a security device as if I bought the domestic DES and I was an American citizen?

Mr. WALKER. We have not—in the ones that we have tested, we have found that these are legitimate DES, just as effective as any DES implementation within the United States. Yes, sir.

Mr. GEJDENSON. So if I were to—if I were to take all of these and have them examined and I was a bank, they would be just as good to me as an American DES product, not the other software part, but security part?

Mr. WALKER. The DES implementations that we have looked at are as good as any, yes. We haven't looked at all of them. There are 200 products here.

Mr. GEJDENSON. Right.

Can you give me three products or four products that you are confident—or one product is all you need, I guess, but if you have three or four that you are confident are of a quality equal to ours?

Mr. WALKER. I would certainly recommend the Algorithmic Research Limited from Israel. Dave Balenson, who is my expert on this, has worked on that, takes them home and plays with them all night. He says they are good or better than anything we could find.

Mr. GEJDENSON. Can we borrow those for a couple of days?

Mr. WALKER. Yes.

Mr. GEJDENSON. What does he do with all of these things when he plays with them? Is he here?

Mr. WALKER. He is right there, yes.

Mr. GEJDENSON. All right. Everybody has a good time in a different way. We live in a democratic government.

Mr. WALKER. The products that we have obtained from these manufacturers are, in every case, first rate implementations of DES.

To better understand this question of, are they somehow inferior, which means being sold overseas, we went to the Sophos distributor in Bahrain and asked if we could get the product that he is distributing in the Middle East.

We were told by the distributor that everything he sells is shipped directly from the manufacturer in England. We already obtained it from England, so we didn't bother.

The uti-maco——

Mr. GEJDENSON. If you were going to get that in Bahrain, would you have to—would the Bahrain sales distributor—when he sent back to England to get it, would the English company need an export license to send it from the English company to the Bahrainian customer?

Mr. WALKER. I will address that in just a minute. But, in fact, the answer apparently is no. If there is anything he needs to do, he fills out a form and says this is a friendly country so I am shipping it, it appears.

The uti-maco distributor from Germany in Connecticut shipped us his product within a day. I asked him if there was, in fact, anything he had to do to go back to Germany to get approval for shipping and he said, absolutely not.

I asked him if that was true elsewhere in the world, and he said he only distributes in the United States, but as far as he understands, nothing is needed to go back to the parent company to get approval. Very different than the situation we have in the United States. We have no indication that the products being shipped to the United States or the rest of the world from foreign manufacturers or distributors are in any way inferior to the products we have in the United States. In many cases, they are substantially better.

But the results of our survey point to a much more ominous finding, the one that you were just referring to: Apparently the controls imposed by the U.S. Government on export of cryptographic products from the United States are far more restrictive than those imposed by most other countries, including our major allies. The effect of this is most unfortunate in that it cripples the U.S. industry while our friends overseas are essentially free to export as they wish.

The United States imposes very strict rules on the export of cryptographic material. We have already heard about some of that. In general, shipments even to friendly countries, unless they are for financial use or for U.S. subsidiaries will be denied. We have been told repeatedly by the government that other countries such as the United Kingdom and Germany have export rules that are just the same as ours. But our experience has shown that to be very different.

Companies in the U.K., Germany, Denmark, and Israel can freely ship DES products to the United States and presumably anywhere else in the world with no more than a few days of government export control delay, if any.

Based on our experiences to date, I conjecture that these countries are using the CoCom, the Coordinating Committee of Western Nations and Japan, rules for determining where to allow exports.

The chart that is just being put up shows in red the CoCom proscribed countries and a set of terrorist countries. All of the countries in green are apparently available for export with minimum restrictions.

So if you are in the U.K. or in Bahrain or in Germany or in South Africa and you want to ship, as long as—it appears—we cannot find this absolutely in fact—but it appears these people can ship with very minimal involvement to any of the countries in green.

Up in the upper left-hand corner, I have a small chart that essentially shows the U.S. view of that. The United States, you can ship to the United States and to Canada, and that is it. Every experience we have with our survey supports this supposition.

Now, whether my theory is correct or not, my experience with these——

Mr. GEJDENSON. Let me just interrupt you again.

Mr. WALKER. Yes.

Mr. GEJDENSON. How can we, operating under CoCom's rules, living in a world where the British, the French, and others—the Israelis are not part of CoCom, so they are not expected to follow those rules, and other countries are not obviously part of CoCom, can't be expected to follow those rules—but for CoCom countries, how can it be that the United States feels that it can only send to the United States and Canada, whereas England, according to your map, can send to virtually the entire free world—well, more than the entire free world, almost the entire non-Communist world?

Mr. WALKER. I don't understand that. The individual countries have their own lists of who they can ship to.

And it appears that in England and in Germany and in Israel and in Denmark, they can—if you call up in England, they will ship you, Federal Express, that night, a product involving DES.

So, you know, you can go to the Internet and get it. But you can call up and order it, and for $200 you can have the product the next day. There is no way—I mean you heard what we were talking about before: Was DES just for authentication, just for financial use. This is full DES, for encryption, for confidentiality purposes.

So I think you have the gist of the point, that I think the rules are different that are being enforced in these other countries.

And to be sure we understand that we are not talking about a few isolated products that involve encryption, more and more we are talking about major information processing applications of the sort we are talking about here that are being demanded as a basic level of security by multinational companies.

Also today we have over here, between the charts, a number of products manufactured by—or for AT&T for sale in the United States and, in some cases, overseas. These are telephone security devices, facsimile communication devices, and data communication devices.

Mr. GEJDENSON. You mean behind your charts?

Mr. WALKER. Yes. We can take them down.

Some of the devices are intended to be made with the administration's clipper chip whenever it becomes available. But all of them are available now, either with DES or with the proprietary encryption algorithm.

Some of the devices are manufactured in Switzerland. They are imported into the United States for sale here, but they cannot be exported. If they break, they cannot be returned to the manufacturer because they have an encryption algorithm that can't be exported.

Mr. GEJDENSON. So what you are saying is if they buy—this makes no sense at all. But we have done other things like that in the past, so this wouldn't be an isolated incident, obviously.

If an American company buys an encryption device for their phone system as those last three things—they are made in Switzerland?

Mr. WALKER. That is right.

Mr. GEJDENSON. AND IF THEY BREAK DOWN, THE ONLY THING THEY CAN DO IS BUY A NEW ONE, THEY CAN'T SEND IT BACK TO SWITZERLAND FOR REPAIR?

Mr. WALKER. I am told that that is, in fact, correct.

Mr. GEJDENSON. Unless they get an export license.

Mr. WALKER. It is encryption for confidentiality purposes, and it is not going to a subsidiary, a U.S. subsidiary, and it won't—it will be denied. In the current rules, they will be denied. I mean it is a crazy situation. What we are finding with all of these foreign products——

Mr. GEJDENSON. I am sure the National Security Agency would not support anything that even remotely looked like a crazy situation. So there must be some misunderstanding here.

Mr. WALKER. There must be something else to it.

Mr. GEJDENSON. Maybe in secret session they will be able to explain it to us.

Mr. WALKER. I certainly hope so.

Mr. GEJDENSON. So do I.

Mr. WALKER. What I would like to do now is give you a brief demonstration of things that can be done with the cryptography that you just saw imported from overseas and how easily that can be implied to protect sensitive information.

We thought about building a demo that would transfer files back and forth, but we decided to use some new national information infrastructure software which, in fact, involves two commercially available computer workstations, one over here will be the transmitter—there is a tape player next to it—and the other one over here will be the receiver.

They are communicating.

We don't actually need the lights off.

Mr. GEJDENSON. Oh, OK. Well, she is gone for a while. Do you want to put the lights back on?

Mr. WALKER. The first thing we are going to do is show some software that is routinely available and being used on the Internet all the time now for voice conferences. In this case rather than speaking, we are going to play you some Mozart for you.

First you will hear it here, and then you will hear it there. What is happening is, the voice is being digitized, compressed, packetized, sent over an internet wire that runs across here but could just as easily go around the world and show up over here. There is a slight delay that we are emphasizing for purposes of the demonstration. All of this is commercially available. Anybody can do it. Your laptop soon will be your telephone. You will speak into it, and it will talk back to you.

Now, the advantage that we have, because this is all being done in software, is we can add DES to it. And so what we are now going to do is take a DES algorithm that we obtained from Australia which we cannot export back, and we are going to impose it on both sides. We will pause here briefly.

Oh, I am sorry, it has already been done. You have been listening to DES protected audio from Australia.

Now, if my friend Dave here didn't want my friend Pete here to be able to hear his music, he could change the key, and he will do that now. And you will hear what an interceptor might detect.

This is improperly keyed DES.

Now, let's put it back.

Now, it takes a few seconds for it to resynchronize. But you can hear the delay.

Now, if you don't like Australian DES from down under, we figure we go as far away in the world as we could and bring you some Swedish DES. So we will now put Swedish DES up.

We could have put the DES that my friend got from Germany here up. It sounds remarkably the same because it is the same. There is no difference.

The point here is that anyone with elementary understanding of a modern computer workstation can do what we have done. There is nothing——

Mr. GEJDENSON. I guess the central question is: Is it any easier for people who want to listen in, who aren't at the two-end terminals.

Mr. WALKER. This will be much more difficult for the people who want to listen in.

Mr. GEJDENSON. Right. But is this somehow inferior DES, so that there is some way that is easier——

Mr. WALKER. Absolutely not.

Mr. GEJDENSON [continuing]. For our intelligence or other intelligence agencies to listen in?

Mr. WALKER. I believe a DES implemented—we have already talked here about NIST validating implementations of DES. These versions of software will pass the NIST validation. These are foreign implementations.

Mr. GEJDENSON. How do you know there are trap doors in these?

Mr. ZIMMERMAN. If you have seen one DES, you have seen them all.

Mr. WALKER. You could have a trap door for example that took the clear text and sent it off to another file. But we are running these programs on workstations. We understand that this program that does DES is allowed this input stream and that output stream. It is not allowed any other output streams. If it tried to output a clear text version of this for some foreign intelligence organization to pick up, it would be just thrown out by the computer system, because it is only allowed a single input stream and a single output stream.

Mr. GEJDENSON. So if I were to tap into this and I were some nefarious organization, not an American organization, but a nefarious organization, and you were doing this from the United States back to a terrorist cell in Libya——

Mr. WALKER. It wouldn't work.

Mr. GEJDENSON. Why wouldn't it work?

Mr. WALKER. Well, how would you get it out? The program that they have there says, take the result of the digitization of the voice, use that as an input stream to the DES software package, use the output of that to go to the packetizing thing to send it across the net.

If there was another output stream, there is no place for it to go.

Mr. GEJDENSON. No. I am assuming that the bad guys have bought this DES and they are now communicating between their cell in the suburbs of Washington, D.C. and their cell in Tehran.

Now the fact that this is foreign DES, would be just as difficult to crack as the DES that the gentleman to the right of you would sell me?

Mr. WALKER. Yes.

Mr. GEJDENSON. No different? How can you prove that?

Mr. WALKER. I am sure that someone could produce a DES that would be inferior in some way. The ones that we have examined, the one in the Israeli product, for example—the ones we are using here are——

Mr. GEJDENSON. You can check and make sure there isn't some other system put in there?

Mr. WALKER. Yes.

Mr. GEJDENSON. And say that confidently?

Mr. WALKER. I can say that in great confidence, yes, sir.

Mr. OZZIE. When you buy a commercial product, you are sort of trusting the company that you buy it from. But what I downloaded was the source code. And the source code is clearly implemented. It says that it was implemented from an algorithm in Dennings Brook, and it shows exactly how it is. You can inspect how they implemented—how they wrote the program.

Mr. GEJDENSON. And so this guy over here that spends his nights looking at codes instead of going out on dates would be able to figure this out?

Mr. OZZIE. Give him a lot to look at and he could figure it out.

Mr. GEJDENSON. You couldn't get anything by him?

Mr. WALKER. It is not hard to test.

Mr. GEJDENSON. OK.

Mr. WALKER. I really am taking a good bit of time.

I would like to tell you just briefly what my experiences have been with my company in this arena.

In my written testimony, I have listed the experiences of a number of companies from the SPA that they have put together. But I would like to tell you my own company's experience with a product called Privacy Enhanced Mail. You are going to hear about Pretty Good Privacy in a few minutes. This is another version of privacy for electronic mail.

PEM is a software product that works with electronic mail packages to add encryption services for secrecy and authentication. PEM is capable of using a wide variety of encryption algorithms. But in the version that is being used on the Internet today, it uses DES and it, therefore, cannot be exported except to Canada.

We have been discussing the use of PEM with the British Government for several years. We have a product that could already have been in wide use there, satisfying their unclassified electronic mail protection needs, but we can't export it.

Last year the SPA, in a very significant accomplishment, negotiated an agreement with NSA that would allow the export encryption products for confidentiality so long as they had a short key, 40-bits or less.

Well, we implemented a version of that, because it is another algorithm that we can use; and we went to our British friends and said, here, now we can sell you PEM. Well, they got DES available, 56-bit in England—it is at 65,000 times stronger than the 40-bit key which we have—and they said politely, we don't even consider such a weak product. They are not interested in that at all.

In fact, I don't know if anybody is interested in the 40-bit key product.

Mr. GEJDENSON. Was this exchange verbally or in written form?

Mr. WALKER. Primarily verbally, unfortunately.

But to attempt to satisfy our British customers, what we had to do is resort to hiring British scientists to take the international specification for PEM, which was written by scientists all over the world, to take the DES algorithm that is available in England and essentially reimplement a completely independent version of PEM there.

The impact on us of that is that, first, we have to pay for the reimplementation of it. Secondly, though—we see immediate loss to the United States of sales of approximately 10,000 systems, roughly $2.5 million over several years—for our company, that represents anywhere from 15 to 25 percent of our revenue over any particular year.

But the most ironic part of this is that because of the apparent differences between the U.K. export procedures and those of the United States, we may be able to import the U.K. privacy enhanced mail into the United States for sale here and, thus, we don't need our PEM operation at all any more; we will just move the operation over there.

Unfortunately, we can't move U.S. citizens there. We have to hire British citizens. If we moved U.S. citizens, that would be an export, and we would be in trouble.

So, unfortunately, these experiences are not at all unique. And similar, and even worse, stories abound throughout the United States.

In conclusion, let me say that, why is all this happening? Well, the U.S. law enforcement, NSA, national security interests, are trying to retain the ability to intercept the communications of our adversaries in the face of accelerating technology shifts that will make it ever easier for those who wish to protect their communications to do so.

I think the demonstration in audio here provided an effective measure of that.

I don't wish to deny the government the right, indeed, the responsibility to try as hard as they can to maintain that ability to listen in to our adversaries, but we must recognize the total magnitude of this problem. We must find a way to balance the costs to the U.S. citizens of losing its vital industrial secrets to foreign espionage and its dominant position in the information processing industry to foreign competition versus what I believe is the inevitable reduction in our intercept capabilities when foreign availability of cryptography is already so great.

So what do we do? The National Research Council has warned about this problem in four recent reports that are available on the table over there and are summarized in attachment 3 of my testimony.

The Computer Systems Security and Privacy Advisory Board called for a national review of this dilemma for almost 2 years. That is attachment 4 in my testimony. The President on September 16 said in commenting about NAFTA, we cannot repeal the force that is driving the world economy together. We can run away from it and get beat by it, or we can embrace it and do what we have to do to win with it.

On September 30, as was mentioned in the opening, the President announced the dramatic relaxation of export controls on all types of computer products. Isn't it time to look at exports and cryptographic products too? If we don't, the national information infrastructure will very likely get its security protection from foreign sources.

We need to recognize that the U.S. public has the right to a reasonable level of protection for its sensitive information enabling that right through allowing the export of good quality cryptography, such as DES, will not harm the intelligence gathering capabilities of this country any more than the worldwide proliferation of cryptography already has.

I strongly urge this subcommittee to press vigorously for legislation to allow the export of good quality cryptography so our computer industry can build this into our products and our citizens can use it to protect their vital sensitive information.

Thank you.

[The prepared statement of Stephen Walker appears in the appendix.]

Mr. GEJDENSON. Mr. Zimmermann

STATEMENT OF PHILIP ZIMMERMANN, CRYPTOGRAPH CONSULTANT

Mr. ZIMMERMANN. My name is Phil Zimmermann and I am a software engineering specializing in cryptography and data security.

A couple of years ago I published a program called Pretty Good Privacy, or PGP. I published it as free software or freeware domestically within the United States and like most free software, it spread organically around the United States to thousands of Americans and sometime after that, it appeared in the hands of people in Europe and other parts of the world.

It has since become the de facto world standard in encrypting electronic mail or at least some people think it has.

I would like to talk a little about the historical context of how this problem of—how these export controls, how they are hurting things here. Historically people have not had accession to good cryptography. The reason why is historically there were no computers around except a few computers in the hands of governments. Also cryptography was not practical for the average person because of the problem of key distribution.

If you want to send a message to someone else, you have to tell them what the key system is so they can decrypt the message with the same key you started at your end. That is not easy for the average person. The governments can do it because they can send somebody carrying a key maybe to their embassies overseas in a black bag, handcuffed to their wrist, but if you want to talk to your cousin in New Jersey, it is not an easy thing to do. So practical cryptography was just not available to the average person.

Two breakthroughs have occurred since that time. One is the cheap ubiquitous availability of personal computers, modems, the Internet, electronic mail, the information age. But with that information age comes an erosion of our privacy.

Before computers came along, our mail was paper mail, only paper mail. It still is mostly paper mail, but with paper mail the government has to target someone for investigation to open their mail or whoever wants to open their mail, a business rival or anyone who wants to read their mail.

This is like going fishing with a hook and a line, catching one fish at a time.

With electronic mail in the information age, more and more of our mail traffic is converting to electronic mail traffic. This means that a larger percentage of our ordinary communications is becoming electronic and easily intercepted.

Government computers or the computers of domestic corporate rivals or foreign corporate rivals or foreign governments can intercept our electronic mail and read it, scanning it automatically for key words. This is like drift net fishing, and this changes the complex of democracy.

If you want to protect electronic mail, you have to use cryptography and to use cryptography requires this second breakthrough in the late 1970's, the invention of public key cryptography. With public key cryptography you can communicate securely with people you have never met without the prior exchange of keys through a secure channel.

This means that ordinary people can communicate with other ordinary people without having to send any couriers carrying keys in black satchels. It means it is as easy as picking up the phone and looking up their number and dialing it, or just sending them some electronic mail without having anything worked out in advance. That makes cryptography available for the great masses of people.

So the convergence of these technologies, the trappings of the information age, personal computers, modems, the Internet, the national information superhighway, all brings together all the parts necessary for everyone to use cryptography. It is no longer just the tools of the military or governments, or for diplomatic traffic. Technology is overtaking us, and if we want to have a global economy, if we want to be able to compete and participate in a global economy, we need to use the trappings of the information age and we cannot do our commerce without digital signatures and that is part of public key cryptography as well.

We need to have cryptography for our privacy. People need their privacy. People want their privacy. That is part of the reason why my product has become so popular.

Trying to legislate this away or regulate it away in State Department regulations is like trying to regulate the tides and the weather. It is like the buggy whip, manufacturers trying to stop cars even with the NSA on their side, it is still impossible.

The information revolution is good for democracy, it is good for a free market, and it contributed to the fall of the Soviet empire. They cannot stop it either. We don't want to be like them, supposedly we are different from them.

As you have just seen in the demonstration here, soon every multimedia PC on the planet will become a secure telephone using just software, no special hardware. It is not like trying to control atomic bombs, which require expensive uranium hexafluoride gas center fumes or plutonium separation apparatus. You don't need that stuff. Anybody can just write encryption software anywhere on the planet and they are doing it.

When I wrote PGP, I used available technology, available methods that were published in the open literature. I published it for the good of democracy. Not to make money, but just for the good of democracy. There is an intimate relationship between the health of a democracy and the ability of the citizenry to conduct private communications. Privacy is part of the American culture. It is a right.

Mr. MANZULLO. Would you yield for a question?

I guess the bottom line here is very simple. Do you feel that we are moving toward an information system which will no longer be able to speak in secret codes and everybody will know what everybody else is doing?

Mr. ZIMMERMANN. If we follow the initiatives launched by certain elements of our Government in law enforcement and intelligent interests of our Government, we may be building an information infrastructure that prohibits private communications and in our preelectronic age society we could easily get private communications by having face-to-face conversations or maybe just sending paper mail.

But because our society is irrevocably changing in the direction, almost all of our communication is happening electronically instead of with paper or face-to-face communication, we are losing our privacy. It is hemorrhaging. We are losing our privacy and people know this. People sense this. And they——

Mr. GEJDENSON. What I will do is ask you to try to be briefer so that we can have the last speaker before we have to go to a vote, and then what we will have is the ability to sweep the room before the NSA answers all these questions in secret.

Mr. ZIMMERMANN. One thing I would like to say quickly here is there has been so much talk on this panel about exporting the DES. Now, Michael Wiener of Bell Northern Research presented a paper at the recent Crypto 1993 conference in Santa Barbara.

At that conference this paper showed how the DES could be cracked for $1 million in 3½ hours with a special purpose machine. He has designed and tested the chip on his CAD system and fully debugged the chip, but he has not fabricated the chips. He can get these chips manufactured for $10.50 each, and can put 57,000 chips in a special machine that could break the DES key in 3½ hours. For a hundred times as much money, for $100 million, you can break the DES in 2 minutes. The NSA budget is even bigger than that.

As word of his results spread throughout the crypto community, you can be sure that the reaction of the world business community is going to be that DES is dead. DES is essentially useless for serious data security applications and we are going to see all of our overseas rivals switching to triple DES, which is a variation using twice as many bits in the key and takes far longer to crack.

That means that if Congress acts now to enable the export of full DES, it is going to be a day late and a dollar short in doing so. Where if we do enable the export of full DES, by the time that happens, all of the overseas rivals will be doing it with triple DES and we will still be in the position we are right now.

We have to allow the export of as much cryptography as people feel like writing.

I want to say one thing about the benefits of privacy. Today, human rights organizations are using PGP to protect their people overseas. Amnesty International uses it, and the Human Rights for the International Advancement of Science uses it.

You talk to people from Eastern Bloc countries, and they don't understand why we do not worry about government power and why we don't value our privacy as much as they do.

They came out of a police state recently and they don't want it to happen to them again. They use PGP. I will read you a quote from electronic mail I got last week from somebody in Latvia. This was at a time on the same day that there was all this fighting in Moscow.

He says, "Phil, I wish you to know, let it never become, but if dictatorship takes over Russia, your PGP is widespread, from Baltic to Far East now, and will help Democratic people if necessary. Thanks."

Mr. GEJDENSON. Thank you.

[The prepared statement of Phil Zimmermann appears in the appendix.]

Mr. GEJDENSON. Mr. Harbert.

STATEMENT OF DON HARBERT, VICE PRESIDENT, SOFTWARE ENGINEERING, DIGITAL EQUIPMENT CORPORATION

Mr. HARBERT. I am Don Harbert, vice president of Software Engineering Digital Equipment Corporation. Thank you very much for the opportunity to be here. I will be brief.

My full text has been entered into the record. I will summarize here and I will speak as quickly as possible.

Digital is a leading supplier worldwide of networked computer systems, software and services, and leads the industry in interactive distributed and multivendor computing. We are an international company. We derive approximately 65 percent of our revenue from outside of the United States.

We produce both encryption hardware and software, and we use a variety of data security products based on this technology in our own networks.

U.S. export controls on encryption products must be brought into line with reality. Many existing controls are ineffective and no longer enhance national security objectives in any meaningful way. These controls do, however, encourage the development of encryption products outside the United States. We have heard ample evidence of that here today.

And the restrictions needlessly deprive U.S. companies of significant export opportunities in some of America's largest overseas markets. It is time for serious reexamination of controls on encryption.

The market for encryption products both outside and inside the United States is significant. In general, any group that employs data communications and is dependent on valuable proprietary knowledge is vulnerable to unauthorized access to that information.

Commercial activities requiring encryption includes banks, and nonbanking industries with a history of industrial espionage such as automobile, petrochemical and pharmaceutical industries. Guides, manuals, and other instructional materials dealing with encryption as well as software packages themselves containing encryption functions are common fare in retail software outlets in the United States, Europe, and elsewhere around the world.

While a limited number of encryption applications are under the jurisdiction of the Department of Commerce, most file or data encryption is subject to control under the Arms Export Control Act administered by the Department of State.

Software containing file encryption, including software in the public domain, or that is called mass market by the CoCom definition, is subject to the same severe licensing regime as are tanks and missiles.

The export licensing regime for munitions administered by the Department of State is even slower, more restrictive and more cumbersome than that for commercial products administered by the Department of Commerce.

An even more important problem, however, is a policy of licensed denial for nonbank commercial customers. The National Security Agency reviews export licenses and sets policy for the export of encryption products. NSA routinely recommends denial of exports to commercial customers, even those located in America's closest allied countries.

And with the exception of a small number of weak encryption products, NSA will approve exports of file encryption products to only nine allied governments, banks, and subsidiaries of U.S. companies.

Thus, not only are these products subject to harsher controls, but there is a de facto embargo of them to America's major commercial data processing markets in Western Europe and Japan. In part, as a result of NSA's embargo policy, a data security industry has developed overseas free from competition from U.S. companies, and completely free from U.S. export controls.

Export controls do exist on encryption products among all of America's major allies, however, but the nature and the severity of controls varies significantly. It is very important to note, with the exception of France, none of the major allies of the United States impose restrictions on the use of encryption within their own borders.

As a result, data security markets within these countries are guaranteed to local producers because of the NSA imposed embargo of products of U.S. producers.

Encryption controls impact the computer industry in many ways. The following cases I will discuss demonstrate the major impacts of current controls on the industry. First, the situation for leveraged sales.

For many large computer companies, like Digital, some large sales are dependent on our ability to offer encryption as a feature of the customer's solution, incorporating hardware, software, and services. Thus, if we are unable to offer an encryption solution, significant loss of revenue may result, even though the encryption, hardware, and software element of the deal may be minor.

Typical examples include replacement of corporate data systems, infrastructure projects, such as PTT installations and cellular telephone network operations. For such projects for overseas customers who perceive data security as necessary, they will be forced to look to non-U.S. vendors for the entire project.

Digital has been directly and negatively affected by an inability to offer file encryption as an element of large integration projects overseas. Over the last 12 months we have lost up to $70 million in contracts from Western European customers because of our inability to deliver encryption as a part of the total solution.

Next, public domain software. The U.S. Munitions List control software containing file encryption even if it is in the public domain, i.e., generally available to the public, as a result, a number of products are available and widely distributed on international networks as we have seen.

Companies like Digital, which access public domain software for internal research purposes, must screen thousands of public domain software applications for encryption in order to keep the encryption out of our international networks and so avoid unintentional export compliance incidents.

In the area of mass market software, generally available to the public, it needs no significant support by the vendor and is beyond effective control. These packages are low cost, marketed in the thousands or tens of thousands and move readily across national borders, over international computer networks, and in personal baggage.

Digital recognizes the need to retain some controls on encryption products in the interest of national security. A number of useful changes in the current policy can, however, be made to rationalize the current system. The changes I will outline will allow U.S. companies to compete for business abroad where data security is a factor, but will retain controls on that which is controllable.

First, the United States should shift jurisdiction for controls of dual-use encryption to the Department of Commerce. Encryption has established commercial applications, is widely used in commercial context, and is specifically controlled by CoCom as a commercial, not a munitions item. Commercial control would not preclude NSA participation in the licensing process, but would mean more flexibility in licensing authorization and more likelihood that commercial and economic needs were at least considered in individual export license decisions.

Secondly, the United States should expand categories of overseas customers for whom export licenses may be approved. Export licenses for encryption products, including those based on the data encryption standard, may now be approved to banks in a range of countries.

This policy of approval should be extended to other customers including large multinational firms and governments outside of the approved nine for some applications.

Third, the United States should decontrol encryption software in the public domain. Encryption software in the public domain or which is generally available to the interested public without restriction is beyond effective control regardless of its technical characteristics.

Fourth, the United States should relax controls on mass market software containing encryption. The United States and its CoCom allies have recognized that mass market products are also beyond effective control and, for that reason, have afforded such software much less stringent licensing treatment.

In conclusion, I would like to reemphasize that U.S. export control on encryption must be changed to reflect technological and market realities. Controls that are no longer effective do not contribute to national security. They do contribute to the proliferation of data security vendors outside of the United States, and they do impede the ability of America's leading computer companies to compete in their largest international markets.

It is indeed time for change.

Thank you very much.

Mr. GEJDENSON. Thank you.

[The prepared statement of Don Harbert appears in the appendix.]

Mr. GEJDENSON. Let me ask two quick questions and then we will go on.

Dr. Hendren, did you go to school with anybody we know?

Mr. HENDREN. Yes, sir.

Mr. GEJDENSON. And do you want to tell us who that is?

Mr. HENDREN. President Clinton.

Mr. GEJDENSON. So have you talked to your old classmate about this problem?

Mr. HENDREN. Not about this, sir.

Mr. GEJDENSON. Well, maybe you should get us a letter to the President, and I will make sure he gets it.

Mr. HENDREN. That can be arranged.

Mr. GEJDENSON. Thank you.

Mr. Walker, you worked for the National Security Agency.

Mr. WALKER. When I graduated from college, I worked for NSA for 12 years, yes.

Mr. GEJDENSON. And if what you are saying is so obvious to you and others, why do you think your old friends at NSA are not seeing it quite as obviously as you are?

Mr. WALKER. I don't understand. It is obvious to most everyone in the country who looks seriously at this. I think they are genuinely concerned about their responsibility of listening in to other people. They don't want to see that damaged.

What they don't realize is the damage is already there. It is already being done. That is the problem I see.

Mr. GEJDENSON. Thank you.

Ms. Cantwell, do you want to take the chair; or do you have a question you wanted to ask?

Mr. ROHRABACHER. I will just note for the record that I sympathize with everything I heard today, and if this was 5 years ago, I would be chastising you for wanting to make a profit at some potential loss of security for the United States.

The cold war is over. It is time for us to get on and realize we are living in a post-cold war world. We are on the edge of a new technological world, which is a very small global community and totally interlocked economically.

So I have taken everything seriously, what you have said, we are talking about billions of dollars worth of sales that are being lost. I think this gentleman said in the 3 months time period you lost how much?

Mr. HARBERT. We have had contracts of $70 million and more in the past few months that we could not win.

Mr. ROHRABACHER. $70 million. We heard testimony earlier from this gentleman about, what was it, $6 to $9 billion?

Mr. OZZIE. $6 to $9 billion are at risk right now because that is the fraction of the overall mass market software industry that is at risk.

Mr. ROHRABACHER. That is direct losses we are talking about. We are not talking about other aspects that indeed make America more competitive.

Mr. OZZIE. Right.

Mr. ROHRABACHER. And strengthen your industry, which of course is the foundation for a lot of other industries' competitiveness. So with that said, thank you very much for your testimony.

Ms. CANTWELL [presiding]. I have a couple of questions, I guess, and I want to thank the panelists for being specific about the actual loss in revenue, because I think this is the first time we have actually had some of those numbers and I appreciate the concern and putting those numbers out specifically as it relates to your individual companies, but it is helpful for us today in specifying what the problem is.

I guess I have a question, which we heard a lot about and I am sure we will continue to debate whether DES is DES, particularly those products provided in other countries. But in looking at the demonstration, Mr. Ozzie, you had today, a question comes to my mind in general about Lotus Notes and piracy of software, and could you give me some idea of what our general piracy problems are?

What percentage of your products are we looking at as far as piracy?

Mr. OZZIE. I cannot give you an accurate number on that. The SPA or BSA can give more specific numbers, but I can easily say that conservatively for every copy that is used legally, there is a copy that is used illegally.

It depends on the type of software it is, but in actual fact it is rampant. It is very rampant.

Ms. CANTWELL. So 30, 40, 50 percent.

Mr. OZZIE. Yes, easily. Again, it just varies on the type of software. The type of software we sell tends to be used in larger corporations and they tend to try to stay legal, many large corporations do.

As the software becomes more available for smaller devices, you know, such as these that various people go to a store and buy, the piracy problem gets very rampant. And if you look at game software, there has not been much education that has been successful in the end consumer's mind, children, most trade games that they have running on their computers and they don't understand really that they are violating the law; that they are stealing intellectual properties. It is a rampant problem.

Ms. CANTWELL. So before we get to encryption, we have piracy, and the general public's understanding of the trade of this particular product.

Mr. OZZIE. Yes, there is a big education problem that we have, and I know the Business Software Alliance has done a lot to try to educate——

Ms. CANTWELL. So when it comes to the education of this particular encryption technology, where is that education on this particular product?

Mr. OZZIE. The issue we were trying to get at with regard to this product is that if you have the export laws force us to have two versions of the product, one available domestically and one available internationally, even someone who was not trying to rip you off completely and just steal the product could buy the overseas version of the product and then obtain the U.S. version, and substitute the executables overseas.

Ms. CANTWELL. The only thing on there is a note, is that correct, on the side of the box?

Mr. OZZIE. That is all that is on there and people frequently pick up the diskette and put it in their pocket while they are visiting the home office and it is a big problem essentially.

Ms. CANTWELL. Obviously there is no liability to.

Mr. OZZIE. Well, we definitely have, from my understanding, we are liable for educating the consumer and making sure that they understand that this is not for export. However, we cannot control what they do and, you know, they have to feel like criminals if they do things like take their lap-top out of the country or do things like that because they know they are violating the law and we have no control over this.

Ms. CANTWELL. Thank you. Mr. Manzullo.

Mr. MANZULLO. Thank you. Two of the panelists here, I believe, Mr. Harbert, you mentioned Digital lost about $70 million in contracts during the past year. That is a direct loss of sales to your company; is that correct?

Mr. HARBERT. Those were bids that we were asked to compete on and either could not because of encryption or lost because we could not supply a competitive encryption technology.

There is an even larger amount of money that we choose not to even bid on because we know we are not competitive with the local suppliers because of a lack of the encryption technology.

Mr. MANZULLO. People don't even ask?

Mr. HARBERT. Or they ask and we don't even go through the bid process.

Mr. MANZULLO. There is a study here, by Frost & Sullivan Market Intelligence prepared this for the business software alliance that talks about a demand on the part of manufacturing for the type of technology that you are fostering here this afternoon.

[The study of Frost & Sullivan appears in the appendix.]

Mr. MANZULLO. The area I represent has 980 factories in the town of 175,000. It is Rockford, Illinois. Fasteners, tool and dye. We build machinery that is shipped worldwide.

Can any of you gentlemen here tell me what impact, if any, your suggestions would have upon my congressional district? Nice question, isn't it?

Mr. HENDREN. Well, if it is automated machinery where they are having micro computers drive parts of the assembly, they could end up with parts of any of the security algorithm on that unknowingly delivered as part of the software they may have purchased from a subcontractor, and they could be illegally exporting and not even know it.

Mr. MANZULLO. One of the things that is built in Rockford are the tool and dies, which make the machines that make the machines down the line. These are all driven by computer technology.

Are you saying that there is a lack of securing that system now?

Mr. OZZIE. Not knowing the specific products, it is difficult to say, but the machining, the whole computer-aided industry is moving toward totally computerizing their operations where you start by drawing the picture of what you want to machine on a computer screen and it gets beamed to wherever a milling machine is or something like that.

Some companies, some of the more leading edge companies, like Ford, are doing multinational design where in one country the design will be done and another country the prototype will be done, and another country the manufacturing will be done and those drawings are beamed electronically, and for industrial espionage reasons and things like that, they do like to encrypt that information.

Now, is the software built into the machines? I don't know, but surely that is the direction we are going.

Mr. MANZULLO. Thank you.

Ms. CANTWELL. Are there any other questions by members of the committee?

If not, I think what the chairman has decided is we will recess until 3:50 and that will give time to set up the room and we will resume the hearing at that time.

[Whereupon, at 3:05 p.m., the subcommittee was recessed, to reconvene at 3:50 p.m.)

APPENDIX

PREPARED STATEMENT OF CHAIRMAN SAM GEJDENSON, SUBCOMMITTEE ON ECONOMIC POLICY, TRADE AND ENVIRONMENT

This hearing is about the well-intentioned attempts of the National Security Agency to try to control the uncontrollable. The NSA seeks to restrict the export of software which is sold in the United States on a mass market basis.

You can go into a software store in virtually any mall in the United States and buy this software. The NSA itself acknowledges that if you have a long-distance telephone line and a modem, you can send this software anywhere in the world. If you have a computer and a modem, you can take this software off the Internet anywhere in the world. But NSA seeks to control its sale not only to countries like Iran, but to countries like Taiwan and Singapore, and even to the United Kingdom and France.

Not only must we wonder why the United States seeks to limit sales to our NATO allies and to others in the free world, but why does NSA think it possible? The issue is not whether individuals in these markets will obtain such software. They certainly will. The issue is whether they will get it legally or illegally, and whether they will get it from American companies or from foreign companies.

I do not question the value of the information sought by the National Security Agency. But once it is determined that the dispersion of this software cannot be controlled, then however much we might want to protect our ability to obtain information, it is beyond our means to do so.

Just as in the case of telecommunications, the National Security Agency is attempting to put the genie back in the bottle. It won't happen; and a vibrant and productive sector of American industry may be sacrificed in the process.

PREPARED STATEMENT OF DR. JAMES K. HENDREN, PRESIDENT, ARKANSAS SYSTEMS

Let me first give you a little background on Arkansas Systems, Inc. and our relationship to the topic of export of encrypted software and hardware. Arkansas Systems works primarily in the Finance Industry and concentrates on providing software to improve the effectiveness of payment systems worldwide. This includes the technologies related to Automatic Teller Machines (ATM's), national and international switching of payment transactions, check processing, and the remittance payments of commercially generated bills. Arkansas Systems has customer installations in 39 countries including Southeast Asia, Latin America, and Eastern Europe including Russia. Arkansas Systems, is a 17-year-old company, with about 100 employees, doing around $10 million in revenues per year and with about 40 percent of the revenue being international.

In the Finance Industry, the Data Encryption Standard (DES) algorithm is an international standard for encrypting payment transactions such as ATM withdrawal transactions. And is, as you know, approved for delivery to selected other countries if delivered to a bank. This makes the algorithm readily available both in software and in hardware devices. The biggest problem we have in using DES internationally is the significant (sometimes 4 to 6 weeks) delay time it takes to get the shipment approved. This delays completing projects, and adds to the cost of the project. It produces needless overhead costs associated with the export of both our products and the products of the hardware vendors with which we work. The approval has always been granted for every project with a financial institution in which we have been involved!

When we work with non-depository institutions such as a finance company, and need to use the same industry standard processes; the approval is extremely difficult to get or is not approved at all. Let me give you an example. We were working with an international oil company. They wanted to credit their employee's payroll accounts and let the employees withdraw funds as they needed them via a debit point of sale card wherever in the world the employee might be located. The roadblock that eventually stymied this project was the impossibility of being able to use the DES algorithm on the network due to export restrictions. International Point of Sale (POS) networks run by institutions other than banks are having to use non-standard encryption equipment and therefore cannot interconnect to existing financial networks in accepted ways.

Now, lets discuss the DES algorithm in particular. The mathematical algorithm itself is readily available. We acquired copies from the dollar sale table at a local bookstore in Little Rock, AR and from a published article in Scientific American magazine. Our business oriented programming staff has written three different versions of the algorithm. Each was developed in a very short timeframe, and one of these has been certified by the National Bureau of Standards. Any user anywhere in the world could do this also. Trying to limit such a readily buildable product is rather ridiculous.

I would also like to relate some of our experiences in Russia, working with Russian banks. The security methods available to the commercial world in Russia are very sophisticated and these bankers, in our experience, are much more security conscious than their U.S. counterparts. Our DES method works and most people are happy with the way security is handled in the United States. But we have had difficulty in trying to convince the Russians that DES is good enough. Some of our projects require certifying security plans for financial transactions with the FAPSI (the Russian federal security office). What they look at is much more involved than just using DES. They want to look at RSA and FIAT SHAMIR algorithms and multiple layers of encryption. Again, trying to restrict an old proven technology that everyone is using and that our foreign former enemies consider inadequate is a waste of effort.

In summary, we at Arkansas Systems believe that the export controls on software and hardware containing the DES algorithm is needless red tape that only impedes international commerce and does not preserve any advantage for the United States in any way. The trade association Information Technology Association of America (ITAA) of which we are members also agrees with this position.

I will be happy to respond to your questions.

Testimony Of

RAY OZZIE, PRESIDENT

IRIS ASSOCIATES

On Behalf Of The

BUSINESS SOFTWARE ALLIANCE

THE IMPACT ON AMERICA'S SOFTWARE INDUSTRY OF CURRENT U.S. GOVERNMENT MUNITIONS EXPORT CONTROLS

Before The

ECONOMIC POLICY, TRADE AND ENVIRONMENT SUBCOMMITTEE

FOREIGN AFFAIRS COMMITTEE

HOUSE OF REPRESENTATIVES

Washington, D.C.
October 12, 1993

Good Afternoon. My name is Ray Ozzie and I am the founder and President of IRIS Associates, a software development company employing 40 people located outside Boston. Our principal product is marketed by Lotus Development Corporation as Lotus Notes. Lotus Notes is work group applications software that allows teams of people to securely access, track, share, organize and route information to anyone, anytime, anywhere.

I am testifying this afternoon on behalf of the Business Software Alliance ("BSA"). Member companies of the BSA include: Aldus Corporation, Apple Computer, Autodesk, Borland International, Computer Associates, Lotus Development, Microsoft, Novell, and WordPerfect. These companies account for 71% of the sales of prepackaged PC software published by all U.S. companies.

We are here today to strongly urge you to immediately permit the export of generally available software with encryption capabilities employing the DES algorithm or other algorithms such as RC2/RC4 at comparable strengths (56-bits). Although the Administration is empowered to make such a decision and currently has the issue under review, in the event they decide not to do so then we ask that you include a provision in the EAA reauthorization bill.

We ask you to do so because current unrealistic, unilateral, U.S. "Munitions" export controls on generally available software with encryption capabilities:

- Do not protect our national security, because encryption technology, techniques, programs and products are widely available abroad; and

- Do threaten to cripple one of America's most important and internationally competitive industries because of lost sales abroad and here in the United States.

Specifically, **based on recent research we estimate $6-9 billion in annual revenues to American companies is currently at risk because of U.S. Government export controls** and that this will increase significantly within the next five years!

The Software Industry Is Important To This Country And Will Become Even More So As We Deploy The National Information Infrastructure

Every governmental, academic or industry study during the last five years of key technologies to America's future includes software prominently on the list. Software is characterized by both rapid technological innovation and widespread use in downstream markets. Software innovation improves the competitiveness of other U.S. industries which utilize software products to make themselves more innovative and competitive. The benefits of continuous software innovation permeate repeatedly through much of the economy.

In March, BSA released a study prepared by Economists, Inc. entitled The U.S. Software Industry: Economic Contributions in the U.S. and World Markets. Based on government and industry information, the study reviewed the economic contribution made by America's "core" software industry: prepackaged software; custom computer programming services; and computer integrated design.

The study found that this "core" software industry:

- Was larger than all but five manufacturing industries;
- During the last decade grew much more rapidly than the remainder of the economy (269% in real terms versus about 30% for the economy as a whole);
- Is contributing to the economic life of every state in the nation; and
- Has achieved startling success in the international marketplace.

Despite this recent growth and success, the software industry will become even more important in the future. The digital information revolution is well underway. It will enable everyone to be plugged into, and interactive with, everyone else. Because of the ease, speed, versatility and reliability of creating and transmitting digital information, it will be the preferred pathway for business and commerce and the desired highway for personal and cultural communications.

To make this a reality, the United States needs an advanced National information infrastructure (NII) that will accommodate and facilitate the widespread use of digital information.

The NII will require the use of interactive, interconnected, interoperable, "smart" information machines -- computers -- not the limited purpose, passive, consumer electronics prevalent today. This fundamental change provides American business with an unprecedented opportunity to leverage its lead in computer systems design and computer software to: create new products and new markets; to take back industries such as consumer electronics that have been lost to foreign competition; and create the industrial base which is going to be critical for the next several decades.

The Administration clearly recognizes the importance of what's at stake and has made the NII the hallmark of its technology policy. We commend them for this understanding. To quote from the recently released report The National Information Infrastructure: Agenda for Action:

> "All Americans have a stake in the construction of an advanced National Information Infrastructure (NII), a seamless web of communications networks, computers, data bases and consumer electronics that will put vast amounts of information at users' fingertips. Development of the NII can help unleash an information revolution that will change forever the way people live, work and interact with each other...."
>
> "The benefits of the NII for the nation are immense. An advanced information infrastructure will enable U.S. firms to compete and win in the global economy, earning good jobs for the American people and economic growth for the nation. As importantly, the NII can transform the lives of the American people -- ameliorating the constraints of geography, disability, and economic status -- giving all Americans a fair opportunity to go as far as their talents and ambitions will take them."

Of course, while much of the talk about the information infrastructure revolves around hardware -- wires, switches, machines that plug into the network -- it is essential to understand that what makes the whole system work is software. Fiber optic networks and digital information machines without software are just wires and boxes -- they would be incapable of responding to even the simplest command or forwarding the simplest message. The hardware may be the "muscle" but it is software that is the "brains." Software transforms the raw power of high capacity networks and computers into information systems that help people at work and at home.

Software does this in two ways. First, it helps the user navigate oceans of digital information to locate or create that which is useful or desired. Second, once a decision is made to send or receive information, it is the software that actually "pulls" the information through the computer switches and wires that are the physical network. As communications and computer technologies become more powerful and less expensive, we will expect them to do more for us and software is the key to making it all happen: easily and often invisibly.

Encryption Can Ensure Privacy And Security In Electronic Information World

The computer revolution has fundamentally changed the way individuals and businesses create, store and transmit information. The rapidly increasing use of computer networks, whether within an office, a single corporation, across the country or around the globe, permits individuals and businesses to communicate and transmit information that far exceeds the paper practices of just a few years ago. However, because of the non-physical nature of the electronic computer medium, traditional methods of protecting information and ensuring its authenticity, such as sealing and signing a letter, are of no use. Rather, the protection and authentication must be available as part of the information itself -- by means of encrypting the data, scrambling it using mathematical techniques so that it is extremely difficult for anyone other than authorized recipients to decrypt it. (Very simply the mathematical basis of modern encryption is multiplying two large numbers together to get an even larger number. It is very difficult to factor this product, that is, to calculate which two numbers were multiplied together to get that larger number.)

In computer generated encryption, the strength of an encryption program depends on: (1) the integrity of the mathematical formulas used such that they are not subject to sophisticated mathematical attack (i.e., no "backdoors"); and (2) the length of the encryption formula (the "key") that encodes the message. The key is measured in terms of "bits," or the number of digits, with longer keys corresponding to stronger encryption schemes.

Strengths in this context means how long it would take someone with a computer to identify the key by randomly trying all combinations -- a so-called 'brute force attack". It becomes exponentially more difficult to randomly crack an encryption formula as more digits or bits are used.

Encryption can be done either through computer software or hardware. Thus, the encryption program can be imbedded on a magnetic media, e.g. a floppy disk or a hard drive; burnt into a microchip (microcircuit) that is part of the computer; or placed on a computer accessory device, e.g. a PCMCIA card. Regardless of the medium used, the encryption program gives a series of instructions to the computer to perform the mathematical calculations necessary to encrypt or decrypt the information.

There are several well-known algorithms, or formulas, for encrypting data. Perhaps the best known is the Data Encryption Standard ("DES") which was developed in the mid-1970s and now is in the public domain, has been adopted as a federal standard for the protection of the government's unclassified information, and is widely used by individuals and business. DES is based on the use of a 56-bit key length. Two other proprietary algorithms (RC2/RC4) made available by RSA Data Security, Inc., based in Redwood City, California, offer certain performance advantages and have been widely licensed by practically all major computer software and hardware publishers. The RSA algorithms work with variable length keys so that in this sense they can be made stronger or weaker than DES. Another leading algorithm, particularly used in Europe, is the International Data Encryption Algorithm ("IDEA"), implemented most frequently in the Pretty Good Privacy software routine widely available on the Internet. IDEA uses a 128-bit key. Finally, there are numerous other algorithms that have been developed in-house by companies and individuals that use a variety of key lengths.

Worldwide Demand For Encryption Is Soaring

Two fundamental recent developments have dramatically increased the need for encryption to protect information. First is the widespread availability and use of smaller, more powerful, and less expensive personal computers. Second is the significant increase in computer networks. In short, the world has moved significantly from one of isolated mainframe computers to a distributed computing, client-server, environment. Yet, while the free-flow of electronic information among many users and through ever more complex and numerous networks is among the greatest benefits of the computer revolution, it also leaves unprotected commercial data and personal information highly vulnerable to electronic eavesdropping and tampering.

Companies are understandably wary of having data floating around or distributed or a network computing environment without a high level of security attached. Companies will be unlikely to keep their latest patent application, sales projections, customer lists, accounting data, financial, correspondence or strategic plans in electronic form if their competitors -- domestic or foreign -- can get at it. They will hesitate to communicate electronically with their customers or to pool knowledge and resources to make the best products. Researchers will be wary about ensuring the integrity of their work. Personnel managers will be reluctant to keep employee evaluations if they are not secure.

Thus, the accounting, banking and securities industries are adamant about employing security using encryption not just for actual financial transactions but also for all their communications. In addition, demand among domestic and multinational companies in the petrochemical,pharmaceutical, telecommunications, health care and other industries is extremely high. As the use of computer aided design and manufacturing

(CAD/CAM) becomes ubiquitous, and engineering data is digitized, a much wider range of industries -- from automobiles to semiconductors -- are demanding encryption for data creation, storage and communications.

Similarly, individuals will be extremely reluctant to permit their doctors to store their medical records in computers rather than on paper. They also will hesitate to communicate electronically with the IRS or their bank. They will be less likely to use the NII to shop, renew their driver's license, or correct a problem with their social security. They will worry about sending letters via E-mail to their friends and family. Their concerns about privacy and security are propelled by popular movies such as Sneakers and Lawn Mower Man, fears of computer viruses, and numerous press accounts of computer hackers.

We could even take an example closer to this institution. Electronic communication among House and Senate offices has been limited in part because of widespread concern that unauthorized persons would be able to access a Member's files and tamper with them, perhaps changing legislative positions and financial records.

BSA recently asked Stanford University Professor Martin E. Hellman about the implications of encryption policy on the National Information Infrastructure. A copy of Professor Hellman's report is attached to my testimony.[1] Professor Hellman first reviewed the many advantages fueling the rapid switch from paper-base to an electronic communications, but then warned that information on the NII would be extremely vulnerable to electronic eavesdropping and tampering unless it was encrypted. Nevertheless, Professor Hellman noted that "unless the Clinton Administration reverses existing national policy which discourages the use of encryption, it will get an insecure NII." He pointed out that an insecure NII poses three possible embarrassments:

> "**A white elephant:** just as people do not use postcards for most of their mail, prudent users will refuse to most information to an unsecured NII.

---

[1] Professor Hellman was one of the inventors of the modern "public key" cryptography, which enables secure communication among parties with no previous relationship. Using public key encryption, anyone can send E-mail messages that are "sealed" so that only the intended recipient can read them and "signed" within a company message verifying that it is truly the author who is sending it.

> **A disaster:** careless or ignorant users who trust confidential or valuable information to an unsecured NII will be easy prey to hackers, thieves, spies or other who violate the system.
>
> **Foreign dominance:** foreign companies, operating from countries which do not discourage encryption, could offer a competing, secure service and could put the NII out of business."

In short, there is a clear and present need for encryption that will grown even larger in the future. Business and personal computer users do not want their information read, changed or stolen. They want reliable, affordable, and convenient security for their documents, data bases, electronic mail and other electronically stored or transmitted data. They want data, file and text encryption capabilities.

BSA recently asked Frost & Sullivan Market Intelligence to survey the demand for information security and encryption among Fortune 500 companies in the United States. The survey covered a broad spectrum of industries including manufacturing, health care and financial services. The companies actually interviewed were about evenly divided between those with and without extensive overseas operations. The results confirm what the marketing departments of our member companies have been telling us for some time.

First, the subject is quite sensitive. Indeed, of the 201 companies contacted by Frost & Sullivan, a quarter were sufficiently uncomfortable with discussing the topic that they felt unable to give specific answers to questions.

Second, of those interviewed, more than 90% said that information security was important to their operations and 78% felt that information security was very important.

Third, 90% of those interviewed felt it was important to communicate electronically corporate-wide. However, 78% also stated that it was important to communicate with outside entities -- customers and suppliers -- as well. This is important because it means that it is not enough to simply ensure that American multinational corporations can communicate internally where they are around the world -- they need to be able to communicate upstream and downstream with their vendors and purchasers as well.

Fourth, and perhaps most importantly, almost one-half (46%) specifically stated that data encryption was important to protect the security and confidentiality of information in addition to passwords and access control. Indeed, 37% stated that they looked for the ability to encrypt information as one feature in software they purchase, with another 8% saying that the answer was proprietary so that they could not respond to the question.

A copy of the Frost & Sullivan report, which I will refer to again later in this testimony, is attached.

Current Unrealistic, Unilateral, U.S. Munitions Export Controls Prevent U.S. Companies From Meeting The Demand For Software With Encryption Capabilities

Incredible as it may seem, today the State Department through its Office of Defense Trade Controls, together with the National Security Agency ("NSA"), controls exports of generally available computer software with encryption capabilities as a "munitions" item. Thus, software is subject to the same export controls as are bombs, bullets and military aircraft. Moreover, the reality of U.S. export control policy in this area is the imposition of a virtual embargo on exports of data, text and file encryption software to foreign commercial users, including those located in some of America's closest allies. The only occasional exceptions are very hard to come by case-by-case approval of sales to one of nine allied foreign governments, certain foreign banks, or foreign subsidiaries of U.S. corporations.

The result is predictable. The U.S. has handed foreign companies a competitive advantage. Recent studies have documented the widespread foreign availability of foreign encryption programs and products which indeed place U.S. companies at a competitive disadvantage because they offer DES-based encryption or use other algorithms at comparable strengths.

Now as many of you know, in July of last year NSA and the State Department agreed to relax and streamline export controls for mass marketed software with moderate levels of encryption capabilities. Specifically, the Bush Administration agreed to permit the export of generally available mass market software programs using RC2 and RC4 with up to a 40-bit key length. Moreover, the State Department agreed to grant export approval within seven days for mass market software using these algorithms at the specified bit lengths. (Other proprietary encryption algorithms also could be used and would be reviewed on a streamlined case-by-case basis with a 15 day turnaround time.)

Not surprisingly, NSA argues that industry should be pleased with that action and on occasion even has suggested we are "satisfied." This is not the case.

To begin with, we certainly remember that NSA's action occurred only as a result of your leadership, Mr. Chairman, and the strong support of this Subcommittee in the last Congress during the reauthorization of the EAA. We had talked ourselves hoarse in trying to persuade the Administration to follow COCOM's Spring 1991 decision decontrolling all mass market software -- including software with encryption capabilities. NSA only moved after this Subcommittee, the full Committee and the House adopted a provision specifically controlling all mass market computer software -- including software with encryption capabilities -- under the EAA and not under the Arms Export Control Act.

Substantively, NSA's action fell well short of what the industry needed to be competitive -- permitting the export of generally available software using DES and other algorithms at comparable strengths. Why did industry agree to go along? Because: (1) it was an improvement over what NSA had permitted to be exported previously; (2) as you well know, the prospects for EAA enactment were uncertain given the Bush Administration's opposition to many provisions; and (3) we were strongly encouraged by Congress to reach some accomodation.

It also is important to remember that as part of the agreement, both sides foresaw that the encryption algorithms and/or bit lengths would have to be regularly reviewed to determine their continued suitability given: (1) advances in computing power and speed which facilitates decryption; and (2) the foreign availability of mass market software with encryption which could place U.S. companies to competitive disadvantage. Industry thought at the time that a process had been established by which representatives from the National Security Council and NSA would sit down with industry representatives semi-annually to discuss these issues and to make revisions accordingly. Unfortunately, this has not proven to be the case. The 40-bit key length limitation on encryption does not live up to the perceptions of the marketplace given the widespread availability of foreign alternatives and the scrutiny of cryptographers.

Current "Munitions" Export Controls For Generally Available Software With Encryption Capabilities Do Not Protect National Security

Quite simply, encryption technology, techniques, programs and products are widely available abroad. Trying to prevent the use of encryption abroad by prohibiting exports of generally available software employing good encryption capabilities, is like standing with a finger in the dike as water pours over the top. You are simply, but unsuccessfully, trying to control the uncontrollable.

Consider: a recent study by the Software Publishers Association revealed that there are at least 215 foreign hardware, software and combination products for text, file and data encryption available from 20 foreign countries and which are sold around the world. Almost half employed DES and many of the others used encryption algorithms at comparable strengths. Moreover, it should be understood that these are not "second class" programs or flawed programs. They offer excellent encryption properly done.

Consider: encryption programs and technology is in the public domain. For example, through the Internet computer users worldwide can access DES encryption implementations and simply down-load them onto their own computers for use. Indeed, this afternoon I would like to show you some of the archives of such DES encryption implementations around the world and show you how quickly and easy it is to down-load a program into my laptop for my use. In addition, the recently popularized Pretty Good Privacy (PGP) software program also is widely available for free throughout the world via Internet. PGP implements the International Data Encryption Algorithm, comes with easy to read instructions, is very simple to install, and is simple to use.

Consider: encryption technology is taught in computer courses around the world, is the subject of dedicated periodicals, and is discussed at international conferences.

Consider: any program that is sold domestically in fact becomes available abroad. Generally available software programs with encryption capabilities are sold in thousands of retail stores throughout the country, by mail and over the telephone. You do not have to pass a loyalty test to enter an Egghead Software store; it is not difficult to conceal a floppy disk when leaving the country. Moreover, even this action is unnecessary: anyone with access to a public telephone line and a modem can transmit a program to a foreign computer in a matter of minutes. (I would have liked to show you how easy it is for me to send the DES implementation I just downloaded to someone in Europe -- but it would be illegal to do so.)

Moreover, it is important to note that once a pirated American software program is abroad, any computer acts essentially as a xerox machine making unlimited perfect copies. Thus current export controls simply contribute to the rampant software piracy problem facing American companies. BSA has testified on many occasions that if piracy around the world were to end overnight, the industry's revenues would double! In short, American companies are being forced to compete with pirated copies of their own programs.

For all of these reasons, the COCOM countries recognized in the Spring of 1991 -- two and one half years ago! -- that all mass market software, including software with encryption capabilities, should not be treated as a munitions item and should be controlled as are other dual-use items. In the case of software, this means export under General License.

Yet the U.S. Government has stubbornly and irrationally perpetuated unilateral export controls. Mr. Chairman, as you and Rep. Roth and the Majority Leader and Minority Whip wrote to the President last month, "the United States should only attempt to restrict the export of that equipment and technology which can realistically be controlled. To try to do more alienates those countries whose cooperation is essential for effective multilateral controls." We at BSA could not agree more.

Continued Unilateral Munitions Export Controls Do Threaten To Cripple One Of America's Most Internationally Competitive Industries

American software companies on average earn one-third of their revenues from export sales and this figure exceeds 50% for the larger companies. American companies have achieved a dominant position in the worldwide market for prepackaged or mass market software (a 75% overall market share) because they have been first to market with the programs offering the features users worldwide are demanding. Today, continued unrealistic, unilateral, munitions export controls are directly limiting the ability of America's software companies from offering a feature in their programs which consumers abroad and here at home increasingly are demanding -- encryption.

As Professor Hellman explained in his paper:

> "Export controls limit [the use of encryption by] domestic as well as foreign entities. Along with the shift to a global economy, communications are becoming increasingly international in nature. Just at few people would buy a new telephone that could only be used domestically, market acceptance is limited for secure communications services and products that can only be used for communicating within the United States. American manufacturers are also loath to build high security devices for the domestic market for fear of drawing attention to the poor security of the export version and to avoid duplicate marketing efforts. Foreign software and hardware manufacturers which operate from

> nations with less onerous export controls therefore have a competitive advantage not only in their home country, but also in the US market. The U.S. Government limits the export, but not the import, of cryptographic products."

Today, America's software company face a Hobson's Choice. Either they must incur the time and expense of marketing two separate software products (one for domestic use and one that is acceptable for export) or forego completely foreign sales.

The first alternative imposes additional costs in packaging, promoting and distributing two versions of the same product. More fundamentally, foreign customers know that they are receiving the "crypto-light" version of the program. Results abroad are predictable -- foreign computer users either seek out a pirated copy of the domestic version (thus forcing the American company to compete with itself) or, equally unacceptable, turn to the foreign vendors for products that are not subject to export restrictions.

The second alternative of forgoing foreign sales is extremely problematic -- for both American companies and the United States as a whole. Today American software companies are among the most successful in the international marketplace. To tell these companies to forego export sales is to tell them cut their earnings in half -- and cripple one of America's star exporting industries.

I discussed earlier the Frost & Sullivan market survey commissioned by BSA. Importantly, we directly asked whether the interviewees would consider purchasing foreign software that otherwise had less desirable features if it included encryption capabilities not available in a domestic program. More than one-third (37%) said that they would consider doing so. Interestingly, another 21% were extremely uncomfortable with the question and refused to answer it.

What do these answers tell us? They confirm what marketing representatives in BSA's member companies have been telling us over and over again: they face a competitive disadvantage that is resulting in lost sales and lost sales opportunities. It is a big problem today -- it will be a disaster tomorrow. As the era of digital convergence begins, many entities are in the formative state of purchasing. But once a company buys software, it is difficult to dislodge. Market share lost will not be regained.

We have repeatedly told the Administration that we are losing sales. Our member companies individually, and confidentially, have told NSA -- and some of you -- specific instances of lost sales. The government also can figure out many of these instances for itself -- every time it denies an export license or discourages a company from even filing an application. Understandably, neither I nor other software company representatives is eager to trumpet its market failures -- we prefer to talk about the sales that are made. Similarly, successful companies do not spend a lot of time documenting their failures -- they are too busy pursuing new business. Moreover, none of this captures the lost sales from users who never even approach us because they know it would be futile to ask an American company to meet their encryption needs.

But the Frost & Sullivan survey results do give us the basis for estimating the market that is at risk. The survey found that at least one-third of current sales is at risk as a result of not including the encryption features demanded by customers. In some respects this estimate is probably too conservative: almost one-half said that encryption was specifically important, and if those who refused to answer are also included, then more than one-half would consider purchasing foreign software otherwise less desirable. At the same time, it is reasonable to think that demand for encryption among the Fortune 500 companies may be ahead of overall market demand. Given these conflicting directions, we believe that an estimate of one-third of the market at risk is justified.

Based on information presented in the Economists, Inc. study done for BSA this spring, citing figures supplied by the International Data Corporation and used by the Department of Commerce, in 1991 America's independent software companies and hardware manufacturers sold $39.4 billion of "prepackaged" software (i.e. non-custom, generally available software). This was split evenly between foreign and domestic sales. Together with other estimates based on Software Magazine's compilations, as well as knowledge of industry performance, BSA estimates total American company revenues (i.e. sales less distribution costs) from prepackaged software of around $18-27 billion, again split about evenly between foreign and domestic sales.

This means that approximately $6-9 billion in U.S. company revenues are currently at risk because of the inability of those companies to be able to sell worldwide generally available software with encryption capabilities employing DES or other comparable strength algorithms. Even if only foreign sales are taken into account, there are still $3-4.5 billion in sales at risk. However, we remind people that the survey was of U.S. companies.

Moreover, the amount of revenue at stake will increase dramatically within five years. First, given continuing education about the importance of data security and the ability of encryption to provide it, the increased popularization of the subject, and the deployment of the National Information Infrastructure and the integration with the International Information Infrastructure, we think it is safe to say that at least two-thirds of the market will be demanding software with good encryption capabilities. (Actually, we think this is a conservative estimate and the number will be closer to 80%.) Second, we believe there is likely to be continued strong growth in the demand for software generally. As the Economists, Inc. study shows, for the years 1982-1990 the software industry grew at 269% and the prepackaged sector grew even faster. Even if the industry were to grow at only half that rate (and the truth is that the market, especially abroad, is likely to grow at high rates), we still are talking about total prepackaged software sales by American companies rising sharply.

By failing to act now to liberalize export controls, our government is directly harming the world-wide preeminent position of America's software industry and threatening America's technological leadership in this vital area.

Conclusion

American software companies must be permitted to sell worldwide generally available software employing DES and other equivalent strength algorithms (56-bits). Current controls make no sense given the widespread availability of foreign encryption programs and products and the uncontrollability of the technology. American companies face enough problems in competing in the global marketplace -- we should not be creating needless problems for ourselves as well.

ORAL TESTIMONY

BY

STEPHEN T. WALKER
PRESIDENT
TRUSTED INFORMATION SYSTEMS, INC.

FOR

SUBCOMMITTEE ON ECONOMIC POLICY, TRADE AND ENVIRONMENT
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

OCTOBER 12, 1993

Good Afternoon. I am pleased to testify today about the negative impact that U.S. export control regulations are having on one of the few industries where the U.S. remains dominant worldwide, the information system software industry.

My name is Steve Walker. I am the founder and President of Trusted Information Systems (TIS), Inc., a ten year old small business with offices around the U.S. and in England, specializing in research, product development, and consulting in information security. I am also here representing the Software Publishers Association (SPA) and its members on this most important topic.

The SPA is the principal trade association of the personal computer software industry. Since 1984, it has grown to over 1,000 members, representing the leading publishers in the business, consumer, and education software markets.

My background includes twenty two years with the Department of Defense, at the National Security Agency, the Defense Advanced Research Projects Agency, and the Office of the Secretary of Defense. My last job with the Government was as Director of Information Systems for the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence (C3I).

I have been a member of the Computer System Security and Privacy Advisory Board (CSSPAB), chartered by the Computer Security Act of 1987, throughout its many deliberations on cryptography.

My written testimony describes the national dilemma between, on the one hand, the interests of law enforcement and national security to limit the availability of good quality cryptography so they can continue to listen in to our adversaries and, on the other hand, the rapidly growing interests worldwide of individuals and businesses to protect their sensitive information.

The tension between these forces has been building for years and is reaching crisis stage. But the arguments on both sides have been mostly gloomy predictions of disaster: from the Government if we were to open up exports of cryptography, and from industry if we don't.

I am very pleased today to be able present some concrete evidence that may begin to move this debate from a war of words to the careful analysis of factual information that is so badly needed.

SPA Survey of Available Cryptography

In May 1993, the SPA chartered a survey of the worldwide availability of good quality cryptography. The findings to date indicate that cryptography is available now to essentially anyone who wants it.

[PUT UP CHART 1 # SUMMARY]

Within just five months of part-time effort by a few dedicated people, we have confirmed product literature and in a few cases actual software for 200 foreign products, 123 using the Data Encryption Standard algorithm, the official U.S. and defacto worldwide encryption standard. We have leads that we are confirming on another 64 foreign products, giving a total of 264 products developed and available outside the U.S.

We have found manufacturers of cryptographic products in 21 foreign countries and distributors of cryptographic products in 33 countries throughout the world.

[PUT UP DISTRIBUTORS MAP, EASEL 2]

Most of the major countries of the western world are represented here.

In the course of the survey, we have also confirmed the availability of 241 cryptographic products in the U.S., 142 using DES, and we are attempting to confirm 47 others. Worldwide, we have identified 552 products overall. The names and countries of origin of these products are listed in Attachment 1 of my testimony.

We are continuing to find more products, manufacturers, and distributors on a daily basis. We believe we have just scratched the surface.

We have assembled a set of notebooks that contain the product descriptions of all confirmed products in our database. We also have some of the sources of the information we have used to find these products. In addition, we have several of the products that we have purchased to confirm that good quality cryptography is indeed available worldwide.

Frequently Heard Arguments

There are a series of arguments that are frequently heard from those who wish to justify continued export controls.

The first one is, "Cryptographic products are not available outside the U.S. so U.S. software and hardware developers are not hurt by export controls." We believe our survey results have already proven that statement to be patently false!

A second argument is, "Even if cryptographic products are available, they cannot be purchased worldwide." Our survey results show that this is also patently false!

We have found 366 companies in 32 foreign countries and the U.S. that are manufacturing, marketing, and/or distributing cryptographic products, most on a worldwide basis. The names of these companies are listed in Attachment 2 of my testimony.

A third argument frequently heard is, "Even if the products are available and can be purchased easily, those sold in other parts of the world are somehow inferior to the products available in the U.S." To the contrary, the results of our survey show that foreign products are just as good and in many cases better than many U.S. products.

We purchased products from several sources throughout the world. We ordered DES-based PC file encryption programs for shipment to the U.S. from:

- Algorithmic Research Limited, of Israel
- Sophos, Ltd, of the United Kingdom
- Cryptomathic A/S, of Denmark
- CE Infosys Gmbh, of Germany
- uti-maco, of Germany

We also obtained a similar product from:

- Elias Ltd., of Moscow, Russia (distributed through EngRus Software International, UK. This product uses GOST, the Russian equivalent of DES.)

All the products we ordered were shipped to us in the U.S. within a few days. The German products were sent to us directly from their U.S. distributors in Virginia and Connecticut, respectively. Our experience has been that if there is export approval paperwork required by the governments of these companies, it is minimal and results in essentially immediate approval for shipping to friendly countries

The products we obtained from these manufacturers and distributors were in every case first rate implementations of DES. To better understand if good products were being shipped to the U.S. and inferior products being sold overseas, we ordered the same Sophos product that we already had from their Bahrain distributor. We were told by the distributor that everything he sells is shipped directly from the manufacturer in England.

The uti-maco U.S. distributor in Connecticut shipped us his German made product within a day and without needing any further approval from the German parent company or the German government. Apparently, they have some form of blanket approval for sale to anyone here. I asked if that was true elsewhere in the world and the representative told me, while he dealt only in the U.S., he believed that this was the case.

We have no indication that products being shipped to the U.S. or the rest of the world from foreign manufacturers or distributors are in any way inferior to products available in the U.S.

In many cases the products have proven to be of superior quality, easily comparable with U.S. products.

Others Use Different Rules

But our survey results also point to a much more ominous finding!

Apparently the controls imposed by the U.S. Government on export of cryptographic products from the U.S. are far more restrictive than those imposed by most other countries including our major allies. The effect of this most unfortunate situation is to cripple U.S. industry while our friends overseas are essentially free to export as they wish.

The U.S. imposes very strict rules on the export of cryptographic products. In general, applications for the export of products that use DES will be denied even to friendly countries unless they are for financial uses or for U.S. subsidiaries. We have been told repeatedly by the U.S. Government that other countries such as the United Kingdom and Germany have the same export restrictions that the U.S. does.

But our experiences with these purchases of cryptographic products show a very different picture.

Companies in the UK, Germany, Denmark, and Israel can freely ship DES products to the U.S. and presumably elsewhere in the world with no more then a few days of government export control delay, if any.

Based on our experiences to date, I conjecture that these countries are using CoCom (the Coordinating Committee of western nations and Japan) rules for determining where to allow exports.

This chart illustrates in red the CoCom proscribed countries plus a set of terrorist countries. All of the countries in Green are apparently available for export with minimal restrictions.

If this conjecture is true, it explains why these countries can readily ship to most countries in the free world. I speculate that companies in these countries may be required to fill out export forms but if they can show that the destination country is not proscribed by CoCom or their local equivalent, they can ship without waiting for further government approval.

Every experience we have had with the survey supports this supposition. If only this were true in the U.S.!

Whether my theory is correct or not, our experience with these purchases has demonstrated conclusively that U.S. business is at a severe disadvantage in attempting to sell products to the world market. If our competitors overseas can routinely ship to most places in the world within days and we must go though time consuming and onerous procedures with the most likely outcome being denial of the export request, we might as well not even try. And that is exactly what many U.S. companies have decided.

And please be certain to understand that we are not talking about a few isolated products involving encryption. More and more we are talking about major information processing applications like databases, electronic mail packages, and integrated software systems that must use cryptography to provide even the most basic level of security being demanded by multinational companies.

AT&T Products

We also have a collection of products manufactured by or for AT&T for sale in the U.S. and in some cases overseas. These include telephone security devices, facsimile security devices, and data communications devices. Some of these devices are intended to be made with the Administration's Clipper Chip whenever it becomes available, but all of them are available NOW with either DES or proprietary encryption algorithms. Some of these devices are manufactured in Switzerland. They can be imported into the U.S. for sale, but they cannot be exported elsewhere. Indeed, if they break they cannot be returned to the manufacturer for repair.

Demo

We now have a brief demonstration of just how available cryptography is and how easily it can be applied to protect sensitive information anywhere in the world.

We have here two commercially available computer workstations running commercially available software and connected by a conventional network (or dialup line). They are communicating audio information (in this case from a tape recorder) much as is done daily by voice conferences on the Internet. The delay you hear is being emphasized for purposes of the demonstration. Everything being shown here is commercially available today throughout the world.

[ADD FIRST CRYPTO TO BOTH SYSTEMS]

We can now add a software version of DES from Australia to both the sender and receiver stations to add good quality encryption to the communications.

[PUT INCORRECT KEY IN RECEIVING WORKSTATION]

Now if Dave wanted to keep Pete from listening in to his music, he could change the key used for the encryption and demonstrate what an interceptor might hear.

Next we reset the key so we can communicate again.

[USE SECOND DES VERSION ON BOTH WORKSTATIONS]

Now we can demonstrate this using a Swedish DES implementation. There is no difference in the result.

There is no rocket science involved here. Anyone with an elementary knowledge of modern computer workstations can do what we have done. All of the software is available essentially anywhere in the world. We must not kid ourselves about this being difficult or unavailable!

PEM Experiences

My written testimony lists many of the experiences of U.S. companies that the SPA has collected. I would like to discuss briefly my company's experiences with one of our products, Privacy Enhanced Mail. PEM is a software product that works with electronic mail systems to add encryption services for secrecy and authentication. PEM is capable of using a wide variety of encryption algorithms but in its Internet version uses DES and therefore cannot be exported except to Canada.

We have been discussing PEM with the British government for several years. We have a product that could have already been in wide use there, satisfying their unclassified electronic mail protection needs, except that we cannot export it to them. When the SPA successfully negotiated an agreement with NSA last year allowing the export of encryption products with short key lengths (40 bits or less), we approached the British with an exportable version of PEM Since DES (with its 56-bit key length, 65,000 times stronger than our 40-bit exportable version) is already widely available in the UK, the British politely informed us that they did not want to consider such a weak product.

To attempt to satisfy our British customers, we have recently hired British scientists to implement an independent version of PEM using the published international specifications and UK versions of DES. The impact on TIS involves the cost of reimplementing something we already have, plus the loss to the U.S. of sales of approx 10,000 systems, roughly $2 5 million over several years. This represents a revenue impact to my company of between 15 and 25% of our total revenue in any given year.

But the ironic part of this is that because of the apparent differences between the UK export laws and those imposed by the U.S., we may be able to import the UK PEM implementation for sale in the U.S. and thus eliminate the need for our U.S. PEM operation all together.

Unfortunately, these experiences are not unique to my company. Similar and all too often worse stories abound throughout the U.S.

Why?

And why is all this happening? U.S. law enforcement and national security interests are trying to retain the ability to intercept the communications of our adversaries in the face of accelerating technology shifts that will make it ever easier for those who wish to protect their communications to do so.

I do not wish to deny the Government the right, indeed the responsibility, to try as hard as they can to maintain that ability. But we must recognize the total magnitude of this problem. We must find a way to balance the costs to the citizens of the United States of losing its vital industrial secrets to foreign espionage and its dominant position in the information processing industry to foreign competition versus the inevitable reduction of our interception capabilities. when foreign availability of cryptography is already so great.

Calls for Action

The National Research Council has warned of this problem in four recent reports (see Attachment 3 of my testimony). The Computer System Security and Privacy Advisory Board has called for a national review of this dilemma for nearly two years (see Attachment 4 of my Testimony). The President said, on September 16, that "...we cannot repeal the force that is driving the world economy together. We can run away from it and get beat by it, or we can embrace it, do what we have to do and win with it.'

On September 30, the President announced a dramatic relaxation of the export controls on all types of high performance computer products. Is it not time to look at the exports of cryptographic products, too? If we don't, the National Information Infrastructure will very likely get its security protection from foreign sources.

We need to recognize that the U.S. public has a right to a reasonable level of protection for its sensitive information. Enabling that right through allowing the export of good quality cryptography such as DES will not harm the intelligence gathering capabilities of this country any more than the worldwide proliferation of cryptography already has.
I strongly urge this Subcommittee to press vigorously for legislation to allow the export of good quality cryptography so that our computer industry will build it into their products and our citizens can use it to protect their vital sensitive information.

Software Publishers Association

1730 M Street
Northwest
Suite 700
Washington, DC
20036-4510

Telephone
(202) 452-1600

Fax
(202) 223-8756

TESTIMONY

BY

STEPHEN T. WALKER
PRESIDENT
TRUSTED INFORMATION SYSTEMS, INC.

FOR

SUBCOMMITTEE ON ECONOMIC POLICY, TRADE AND ENVIRONMENT
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

OCTOBER 12, 1993

OVERVIEW 2
WHY DO WE HAVE EXPORT CONTROLS ON CRYPTOGRAPHY? 4
HOW WIDESPREAD IS CRYPTOGRAPHY WORLDWIDE? 7
HOW IS U.S. INDUSTRY BEING AFFECTED BY EXPORT CONTROLS? 13
HOW ARE U.S. CITIZENS AND BUSINESSES BEING AFFECTED BY ALL THIS? 18
WHAT EFFECT WILL CLIPPER HAVE? 18
WHAT CAN BE DONE? 19

Good Afternoon. I am pleased to testify today about the negative impact that U.S. export control regulations on cryptography are having on one of the few industries where the U.S. remains dominant worldwide: the information system software industry. The major points of my testimony are that U.S. export controls do not prevent the international availability of good quality cryptography but do penalize the U.S. software industry and U.S. business in general.

My name is Stephen T. Walker. I am the founder and President of Trusted Information Systems (TIS), Inc., a ten year old firm with 85 employees. With offices in Glenwood, MD; Los Angeles, CA; Mountain View, CA; Minneapolis, MN; and London, UK, TIS specializes in research, product development, and consulting in the fields of computer and communications security. I am also here representing the Software Publishers Association (SPA) and its members on this most important topic.

The SPA is the principal trade association of the personal computer software industry. Since 1984, it has grown to over 1,000 members, representing the leading publishers in the business, consumer, and education software markets.

My background includes twenty-two years as an employee of the Department of Defense, with the National Security Agency (NSA), the Defense Advanced Research Projects Agency, and the Office of the Secretary of Defense. During my final three years in Government, I was the Director of Information Systems for the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence (C3I).

In 1983, I left Government service and began my own consulting firm, specializing in the area of information systems security. My company has experienced steady growth and now offers a variety of products with improved information security for military and civilian applications in addition to our continuing consulting activities. Several of these products are adversely affected by U.S. Government export controls, as are the products of many SPA members.

For the past two years, I have been a member of the Computer System Security and Privacy Advisory Board (CSSPAB), chartered by Congress in the Computer Security Act of 1987 to advise the Executive and Legislative Branches on matters of national concern in computer security. In March 1992, the Board first called for a national review of the balance between the interests of law enforcement/national security and those of the public regarding use of cryptography in the United States. The Board has been heavily involved in this review, receiving public input on the Administration's Clipper Initiative, announced by the President on April 16 of this year. Participation in the Board's review has been highly beneficial in helping me form my opinions in this area.

OVERVIEW

The focus of attention at today's hearing is the negative impact that U.S. export controls on cryptography are having on the U.S. computer industry. In May 1992, I testified before the House Judiciary Committee, Subcommittee on Economic and Commercial Law hearings, on the impact of U.S. export laws on our industry's ability to protect itself from foreign industrial espionage. I also participated in similar hearings in July 1991 and June 1990 in which this topic was of major importance. The export control subject continues to arise in different contexts, but the difficult problems lurking behind it are always the same.

The stakes for the software industry are high. The U.S. holds 75% of the global market for packaged software. Most software companies make 35-40% of their revenue from exports; for some companies exports are as much as 50% of their business. When demand for cryptographic products is increasing, export restrictions essentially place an "earnings cap" on U.S. software publishers.

A National Dilemma

The basic issue is a dilemma of truly national proportions between the long standing and vital interests of our Government to learn as much as it can about its adversaries--be they criminals, terrorists, or other governments--on the one hand, and the basic right to privacy that all Americans assume they have and are seeking to extend to their personal and business communications, whether by telephone, electronic mail, or other forms of computer communications.

The resolution of this dilemma will have enormous impact on our country for decades to come. The Government's national security interests contend that if good quality cryptography were to become widely available in this country and the world, our ability to wiretap criminals and listen in to terrorists and other adversaries would be severely hurt. Those seeking improved privacy protection argue that encryption is needed to support worldwide business operations and good quality cryptography is already available worldwide. Continuing U.S. Government restrictions are only penalizing U.S. users with inferior U.S.-developed security products and limiting U.S. industry from participating in a rapidly growing international marketplace.

Technology Has Shifted

The core of the issue is a shift in technology over the past twenty years that has fundamentally altered both business communications needs and an advantage that law enforcement and national security interests have enjoyed since the earliest days of electronic communications. Before radio and telephone communications, governments had to resort to intercepting mail and notes carried by spies to learn their adversaries' plans. When electronic communications became prevalent, governments found they could intercept those communications relatively easily with very useful results. When encryption was applied to these communications, it became more difficult to make sense of them, but that turned into a test of wits among the mathematicians of various countries. Some were more successful than others.

During the time up to the 1980s, this behind-the-scenes struggle was waged among governments with little if any effect on individuals or business communities. But technology shifts beginning in the early 1980s and accelerating at breathtaking rates today resulted in vast computer communications and security capabilities for industrial and personal use worldwide and at the same time have made it much harder for law enforcement and national security interests to continue their interception roles.

As we struggle to understand the complex issues confronting us in this dilemma, we must recognize that even if U.S. commercial and private interests were willing to forgo their right to private communications and U.S. computer manufacturers were willing to drop out of the international market for information products employing good quality security protection, the ability of the Government to decrypt the communications of its adversaries will continue to diminish at ever increasing rates over the foreseeable future, no matter what measures, such as employing key escrow techniques or outlawing cryptography, our Government may choose to take.

The technology shifts we are seeing here have interesting parallels to those in the field of radar. Since the beginning of World War II, radar has played an essential role in defending against attacks from the air. But recent technology shifts have produced stealth capabilities that for now, at least, effectively defeat radar. We will soon face an equivalent dilemma as stealth measures become widely available: how to prevent drug dealers, terrorists, and other adversaries from using them to enter our country undetected. We could require that all aircraft have some form of reflector that will guarantee that the Government can detect them whenever it has the need, but it is unlikely that those who wish to enter our airspace undetected will comply with such requirements.

We must recognize that those who wish to protect their communications from eavesdroppers will increasingly be able to do so. We must be careful not to continue to insist on misguided measures to try to retain decryption capability that will inevitably be eroded by technology, no matter how important we feel that capability may be.

The Congress Must Act Now!

The principal vehicle that the Government's law enforcement and national security interests have used to maintain the balance on their side of this dilemma over the years has been the imposition of strict export control measures on all cryptographic products leaving this country. In light of the ongoing and inevitable technological shift toward better protection mechanisms and increasing business communications needs, a review of this policy is urgently needed. Such a review must be conducted by someone willing to understand the needs of both sides of the issue. Based on our experiences to date, I am convinced that the U.S. Congress is the only organization with the authority and balanced perspective to tackle such a tough issue. I hope that these hearings will be the beginning of a true national debate of this most vital issue.

I would like to begin my testimony with a review of how these export controls came into place and why they made good sense in an earlier time but not necessarily now. I will then discuss the widespread and rapidly growing foreign availability of cryptographic products that is making this technological shift so hard for our intelligence capabilities. Following this, I will review the highly negative effect that U.S. export controls are having on U.S. industries and the average U.S. citizen.

WHY DO WE HAVE EXPORT CONTROLS ON CRYPTOGRAPHY?

The method that governments have used for most of this century to protect the privacy of their electronic communications and that has gradually become available to individuals throughout the world is called cryptography: the scrambling of data prior to transmission (encryption) and unscrambling upon receipt (decryption).

As governments came to rely upon cryptography to protect their vital communications, groups of highly skilled mathematicians were assembled by the same governments to attempt to break the encrypted communications of their adversaries.

In David Kahn's 1973 book, *The Codebreakers*, he states:

> Codebreaking is the most important form of secret intelligence in the world today. It produces much more and much more trustworthy information than spies, and this intelligence exerts great influence upon the policies of governments.

Few would argue that this statement remains just as true today as when it was written.

Export Controls Were Essential Initially

All modern governments face the difficult competing tasks of having good enough encryption capabilities to protect their own communications while trying to defeat the encryption capabilities of their adversaries. As encryption hardware devices became readily available, governments had to control where these devices went in order to limit the availability of good cryptography to hostile adversaries. Export control on encryption devices became an integral part of the Department of State munitions control process, where it remains today.

With the advent of computers, the ability to perform encryption functions using software programs rather than hardware made encryption more readily available and its export control more difficult. In the 1970s, efforts to improve the protection of domestic sensitive information led to publication of encryption algorithms such as the Federal Information Processing Standard (FIPS) Data Encryption Standard (DES) algorithm, which, while intended to be implemented only in hardware, quickly became available throughout the world in software.

Personal computers gave individual users direct access to the vast power of the computer and led to a revolution in how businesses operate. Now highly sensitive corporate plans and financial information flow freely over the phone lines among clusters of computers, and users are demanding improved security for their sensitive information from their software suppliers.

The natural result of this evolution is the need to include good quality encryption capabilities within modern software products for sale to multinational corporations worldwide. However, governments still want to control where encryption devices go in order to limit the availability of good quality encryption to hostile adversaries.

But Times Have Changed

So a problem that twenty years ago only affected governments and that led to the harsh export control restrictions presently in place on encryption now threatens the ability of U.S. citizens and businesses to protect their own sensitive information and the ability of the U.S. software industry to market the products that its multinational customers are demanding. This is truly a dilemma of national proportions that cannot be left solely in the hands of the national security interests to resolve.

Few would argue that the Government should not continue listening to the communications of its adversaries. But now that we have a worldwide economy with massive amounts of sensitive information flowing in all directions at all times, few are willing to give up the ability to provide reasonable protection to their own information in order to help the Government eavesdrop.

"Listening In" Will Keep Getting Harder

Even if we could forgo our personal and business privacy needs for the sake of the national security interests, the continuous evolution of technology has already made it harder to listen in to those who do not want to be heard than it was even a year ago. And that evolution will continue to make it even harder next year and in every year that follows.

The same technologies that have brought about the personal computer revolution are making good quality cryptography available worldwide, and those people, businesses, and governments that choose to protect their communications can now do so quite effectively and at reasonable cost. The task of listening in to others is becoming more and more difficult every day in spite of extensive export controls.

The widespread availability of encryption products worldwide will make it ever harder to decrypt the communications of adversaries who do not want to be heard, with or without excessive export control measures.

It is important to note that whether the U.S. Government drops export controls altogether on encryption products or attempts to impose absolute restrictions even on domestic use of encryption, the task of law enforcement and the national security community to listen in to our adversaries is going to get progressively harder day by day.

Now Export Controls Are Harmful to the Nation

Export controls served a useful purpose following World War II and up to the early 1980s. They protected the Government's interests and did not interfere with the interests of private citizens and commerce. Since cryptography has become an important tool for protecting the sensitive information of everyone, not just governments, and since the technology to implement good quality cryptography has now become readily available worldwide, export controls on good quality cryptography are no longer needed and are highly detrimental to the interests of the nation.

HOW WIDESPREAD IS CRYPTOGRAPHY WORLDWIDE?

Since the publication of the Data Encryption Standard as a U.S. Federal Information Processing Standard in 1977, cryptography has shifted from the exclusive domain of governments to that of individuals and businesses. DES in both hardware and software implementations is the de facto international standard against which all other algorithms are measured.

DES must be recertified as a FIPS every five years. In 1982, it was recertified without controversy. In 1987-1988, NSA recommended against recertification except for specialized use such as banking, but the recertification proceeded. This year the recertification is before the Secretary of Commerce awaiting approval. If approved, software implementations of DES will be allowed for the first time.

DES was adopted by the U.S. and international banking community shortly after its publication as a FIPS. The banking community fought for and obtained the right to export DES for financial uses, primarily integrity checks but also for banking confidentiality uses, and the right to generate their own keying material (the random numbers that initialize the encryption/decryption processes) without relying on any other Government agency.

In the mid 1980s, DES was proposed as an international standard by the International Standards Organization (ISO) as Data Encryption Algorithm-1 (DEA-1). Final approval was not made because of an appeal by the U.S. suggesting that the ISO should not approve any specific algorithms but leave that decision to individual nations.

The availability of DES and the controversy that arose as soon as it was published concerning whether it had weaknesses that NSA could exploit fostered the highly fruitful academic research into public key cryptography in the late 1970s. Public key algorithms have the major advantage that the sender does not need to have established a previous secret key with the recipient for communications to begin. Public key algorithms such as RSA have become as popular and widely used as DES throughout the world for integrity, confidentiality, and key management.

SPA Study of Availability of Cryptography

The Administration has asserted that export controls are not harming U.S. firms by causing them to lose market shares because there are no foreign products and programs available. Implementations of DES, RSA, and newer algorithms such as the International Data Encryption Algorithm (IDEA), an algorithm that has a key length more than twice that of DES, are available routinely on the Internet from sites all over the world. But according to the Administration, these do not count as commercial products.

In order to develop a definitive assessment of just how widespread cryptography is in the world, in May of this year, the SPA commissioned a study of products employing cryptography. There was a significant amount of knowledge about specific products here and there, but no one had ever tried to assemble a comprehensive database with, where possible, verification of product availability.

The SPA research team focused exclusively on products providing text, file, and data communications encryption capabilities and on programs and products using DES or its equivalent, i.e., the precise products subject to export restrictions. We did not include facsimile and voice encryption products. The team obtained information from product literature, reference guides, industry surveys, trade press and journal articles, and responses to requests for information from SPA members, cryptography experts, and information requests put on the Internet.

Whenever possible, the team followed up information with requests for product literature. This was carefully scanned by at least two independent project members, and the data was prepared for entry into the database. To the greatest extent possible, phone calls have been made to vendors to clarify ambiguous technical information.

Information on new products continues to flow in daily but as of October 12:

- We have identified 264 foreign hardware, software, and combination products for text, file, and data encryption from 21 foreign countries: Argentina (1), Australia (18), Belgium (8), Canada (16), Denmark (14), Finland (1), France (5), Germany (33), Hong Kong (1), India (1), Ireland (1), Israel (10), Japan (2), the Netherlands (15), New Zealand (1), Norway (1), Russia (8), South Africa (7), Sweden (17), Switzerland (18), and the United Kingdom (86).

- Of these 264 products, 123 employ DES.

- We have confirmed the availability of 58 foreign encryption software programs and kits that employ the DES algorithm. These are published by companies in Australia, Belgium, Canada, Denmark, Finland, Germany, Israel, the Netherlands, Russia, Sweden, Switzerland, and the United Kingdom. We know some have distributors in other foreign countries and in the United States; one, a UK company, has distributors in 13 countries (Bahrain, Denmark, France, Greece, Ireland, Italy, Malta, the Netherlands, Norway, Singapore, Spain, Sweden, and Yugoslavia). One in Germany has distributors in 14 countries (Australia, Austria, Belgium, Canada, France, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland, Turkey, the UK, and the U.S.). The programs are installed by the user inserting a floppy diskette; the kits enable encryption capabilities to be easily programmed into a variety of applications.

A complete listing of all confirmed products in the database is identified in Attachment 1.

We have ordered and taken delivery on products containing DES from four countries: Denmark, Germany, Israel, and the United Kingdom.

Foreign customers increasingly recognize and are responding to the need to provide software-only encryption solutions. Although the foreign encryption market is still heavily weighted towards encryption hardware and hardware/software combinations, the market trend is towards software for reasons of cost, convenience, and space.

- On the domestic front, we have identified 288 products, of which 142 employ DES. Thus, at least, 142 products are unable to be exported, except in very limited circumstances, to compete with the many available foreign products.
- In total, we have identified to date 552 cryptographic products, developed or distributed by a total of 366 companies (211 foreign, 155 domestic) in at least 33 countries.

DES is also widely available on the Internet, and the recently popularized Pretty Good Privacy (PGP) encryption software program, which implements the IDEA, also is widely available throughout the world.

The ineffectiveness of export controls is also evident in their inability to stop the spread of technology through piracy. The software industry has a multibillion dollar worldwide problem with software piracy. Mass market software is easy to duplicate and easy to ship via modem, suitcase, laptop, etc. Accordingly, domestic software products with encryption are easily available for export--through illegal but pervasive software piracy--to anyone who desires them.

It cannot be any clearer: the existence of widespread and affordable cryptographic products overseas is an indisputable fact. Based on that fact, unilateral U.S. export controls keep U.S. firms from competing in the global marketplace.

Foreign customers who need data security now turn to foreign rather than U.S. sources to secure that need. As a result, the U.S. Government is succeeding only in crippling a vital American industry's exporting ability.

Following the first publication of the cryptographic database at the Advisory Board meeting on June 2, the Administration requested a meeting with the SPA research team to review their approach and findings. This meeting was held on July 1, 1993, at the Department of Commerce and involved Government representatives from the Department of Commerce and NSA. The team described both their technique for gathering and cataloging the information and the latest results. At the conclusion of the meeting, it appeared that the Administration representatives were satisfied that a valid survey process was being carried out.

At the second meeting of the Advisory Board on July 29, a Government representative of the Administration indicated that the mere availability of products overseas was not sufficient, that what was needed was an assessment of the market impact of those products. It is important to note to the contrary, though, that the Department of Commerce, in similar deliberations, requires only the demonstrated existence of foreign products, not an assessment of their market share. It would seem that no matter how much information is acquired at what level of detail, the Administration will request more to delay further action.

Nevertheless, the study begun in May by the SPA will continue to collect additional information on cryptographic product availability and to periodically publish its results to help focus attention on this important and often ignored situation. We would welcome Government participation in this ongoing effort to ensure the maximum coverage of available products and maximum utility to the Government.

Frequently Heard Arguments

One argument that is frequently heard to justify continued export controls is that cryptographic products are not available outside the U.S. so U.S. software and hardware developers are not hurt by export controls. The statistics from the SPA survey (264 foreign products, 123 using DES) prove that this argument is patently false!

A second argument is that even if products are available, they cannot be purchased worldwide. This is also patently false!

We have found 366 companies in 32 foreign countries and the U.S. that are manufacturing, marketing, and/or distributing cryptographic products, most on a worldwide basis. The names of these companies are listed in Attachment 2.

A third argument frequently heard is that the products sold in other parts of the world are inferior to those available in the U.S. Again, the results of our survey show this to be patently false!

We purchased products from several sources throughout the world. We ordered DES-based PC file encryption programs for shipment using routine channels from:

- Algorithmic Research Limited (ARL), Israel
- Sophos Ltd., UK
- Cryptomathic A/S, Denmark
- CEInfosys GmbH, Germany
- uti-maco, Germany
- Elias Ltd., Russia (distributed through EngRus Software International, UK)

All the products we ordered were shipped to us in the U.S. within a few days. The German products were sent to us directly from their U.S. distributors in Virginia and Connecticut, respectively. Our experience has been that if there is paperwork required by the governments in which these companies operate to approve cryptographic exports, it is minimal and results in essentially immediate approval for shipping to friendly countries.

The products we obtained from these manufacturers and distributors were in every case first rate implementations of DES. To better understand if foreign products are somehow inferior, we tried to order the same Sophos product from their Bahrain distributor. We were informed by the distributor that since we were outside his area, he could not sell directly to us. He then told us that everything he sells is shipped directly from the manufacturer in England.

The uti-maco U.S. distributor in Connecticut indicated that he could ship us his German made product immediately (we received it the next day), without needing any further approval from the German parent company or the German government. Apparently, the Germans have a form of blanket approval for sale to anyone in the U.S. I asked if that was true elsewhere in the world and the representative told me that while he dealt only in the U.S., he believed that this was true.

We have no indication that products being shipped to the U.S. or the rest of the world from foreign manufacturers or distributors are in any way inferior to products available in the U.S.

Others Use Different Rules

But our survey results also point to a much more ominous finding! Apparently the controls imposed by the U.S. Government on export of cryptographic products from the U.S. are far more restrictive than those imposed by most other countries including our major allies. The effect of this most unfortunate situation is to cripple U.S. industry while our friends overseas are essentially free to export as they wish.

The U.S. imposes very strict rules on the export of cryptographic products. In general, applications for the export of products that use DES will be denied even to friendly countries unless they are for financial uses or for U.S. subsidiaries. We have been told repeatedly by the U.S. Government that other countries such as the United Kingdom and Germany have the same export restrictions that the U.S. does.

But our experiences with these purchases of cryptographic products show a very different picture.

Companies in the UK, Germany, Denmark, and Israel can freely ship DES products to the U.S. and presumably elsewhere in the world with no more then a few days of government export control delay, if any. The claim is they have to "fill out some papers," but it's no big problem.

Based on our experiences to date, I conjecture that these countries are using CoCom (the Coordinating Committee of western nations and Japan) rules for determining where to allow exports. If this conjecture is true, most countries in the free world can readily receive exports from these countries. I speculate that companies in these countries are required to fill out export forms but if they can show that the destination country is not proscribed by CoCom or their local equivalent, they can ship without waiting for further government approval. Every experience we have had supports this supposition.

Whether my theory is correct or not, our experience with these purchases has demonstrated conclusively that U.S. business is at a severe disadvantage in attempting to sell products to the world market. If our competitors overseas can routinely ship to most places in the world within days and we must go though time consuming and onerous procedures with the most likely outcome being denial of the export request, we might as well not even try. And that is exactly what many U.S. companies have decided.

And please be certain to understand that we are not talking about a few isolated products involving encryption. More and more we are talking about major information processing applications like databases, electronic mail packages, and integrated software systems that must use cryptography to provide even the most basic level of security being demanded by multinational companies.

Demonstrations of Available Cryptographic Products

We have before us today several examples of cryptographic products that were lawfully obtained in the United States from foreign vendors:

- AR DISKrete: produced by Algorithmic Research Limited (ARL), Israel.
  Uses DES disk/file encryption to provide PC security and access control.
- EDS: produced by Sophos Ltd., UK.
  DES-based PC file encryption package.
- F2F (File-to-File): produced by Cryptomathic A/S, Denmark.
  DES-based PC file encryption utility.
- Softcrypt: produced by CEInfosys GmbH, Germany.
  DES-based PC file encryption utility.
- SAFE-GUARD Easy: produced by uti-maco, Germany.
  DES-based PC file encryption utility.
- EXCELLENCE for DOS: produced by Elias Ltd., Russia distributed through EngRus Software International, UK.
  GOST-based (Russian DES equivalent) PC file encryption utility.

We also have a demonstration of the power of the digital revolution and the impact it will have on all our communications in the future. Traditionally, when we think of voice communications, we think of the telephone in its many forms (desk, cordless, cellular, car). However, many modern computer workstations now have the ability to carry voice as well as other multimedia communications. Routinely today on the Internet, voice conferences are held over packet switched communications networks.

Today we have a demonstration using two workstations that come with software to digitize voice communications, packetize it for transmission over a network, and resynthesize it into perfectly good (sometimes better than phone quality) voice. Systems like these are being used daily for voice conferencing over networks around the world.

With this capability, it is straightforward to protect phone conversations from eavesdroppers. Since all the capabilities are performed in software, it is trivial to add an encryption algorithm, such as the Data Encryption Standard, to the software and provide good quality encryption to the digitized, packetized speech. Today we have DES versions from Finland, Sweden, Australia, and the U.S.

HOW IS U.S. INDUSTRY BEING AFFECTED BY EXPORT CONTROLS?

TIS Experiences

To begin this section, I would like to give several examples of experiences that my company has had recently in dealing with the export control process.

Trusted Information Systems is a member of the Internet community and has implemented a version of the Internet Privacy Enhanced Mail (PEM) system, which it is offering free to users on the Internet and for sale to commercial users under the name Trusted Mail™. Several hundred Internet users have retrieved the PEM source code, and many of them are using it on a daily basis. Our experiences with PEM illustrate the variety of frustrations, confusion, and lost opportunities that confront U.S. businesses in the area of international cryptographic products.

PEM is based on international Internet specifications developed over the past five years by a team of researchers from throughout the world. In its present version, PEM uses DES for confidentiality and RSA for signature and key management. As such, it does not meet the U.S. Department of State requirements for export outside the U.S. or Canada.

In order to establish a distribution system for PEM similar to that of other software products on the Internet, TIS reviewed various techniques that universities and other companies have used. The "anonymous FTP" approach, in which a user who does not have an account is allowed to log on to the computer containing the information and perform a file transfer of the specific program files, was considered the best choice. Such techniques are routinely used throughout the Internet, but in the case of software that is subject to export controls, one must be concerned that individuals outside the U.S. and Canada may attempt to retrieve the programs. The problem is how to identify whether someone who is anonymous is approved to retrieve the software or not.

As had been done earlier by others, we have created a "READ ME" file that the person seeking the software must read before retrieving the PEM program. The reader is cautioned that if he or she is not from the U.S. or Canada, it is against U.S. export law to proceed. The file name of the PEM programs contained in the "READ ME" file is changed frequently to force the anonymous user to read the export control caution. We also installed filters that automatically refuse requests that are clearly coming from outside the U.S. or Canada. But we know that those filters cannot stop inquiries from foreign sources that have accounts in the U.S. To the best of our knowledge, our approach is as sound as many that others are using and better than most.

Before we put the system on line, though, we sought the approval of the Department of State and the National Security Agency. Initially we got acknowledgements to our phone calls describing our problem and proposed solution. We were told orally at one time that because the PEM software was "free," it was permissible to proceed this way, implying that if we charged for it, somehow this process would not be approved. But as we began to seek official approval for this process, we received fewer and fewer responses. Our inquiries finally took the form of: "Unless you tell us not to do this, this is how we intend to proceed." On June 1, 1993, we put the anonymous FTP process on line, and our system has responded to hundreds of requests. We have never received acknowledgement that the process is either acceptable or unacceptable to the Government despite being told on several occasions that we would receive such acknowledgement.

The above described process is patterned after a similar process that takes place now in software retail stores. Programs for sale over the counter containing DES or similar export controlled software are supposed to be marked with explicit and obvious labels telling the buyer that these products cannot be taken from the U.S. or Canada. The burden of complying with the export laws rests entirely with the buyer since the seller has no responsibility to ascertain whether the buyer is a U.S. or Canadian citizen. One has to wonder if these prominent notices, rather than advising buyers to beware, do not guide the foreign buyer, who is not concerned with violating U.S. export laws, directly to the product he or she wishes to buy.

A second situation of interest involves a potential major customer of PEM, the British Ministry of Defence (MoD). For several years, TIS has been discussing PEM with officials in the MoD for use with unclassified information among MoD users and their industrial suppliers. TIS has a perfectly good solution to MoD's problems and could have had it running there years ago. Unfortunately, we cannot export PEM even to the British MoD because PEM uses the DES and RSA encryption algorithms.

Last year, the SPA succeeded in obtaining expedited export approval for software products that use cryptography so long as the key length is 40 bits or less. While this was a significant accomplishment, since it was the first time that any cryptography for confidentiality was given general export approval, the victory was short lived. Forty-bit key algorithms can be exhaustively searched in very short times. If a device could be built to exhaustively search a 56-bit key space (DES) in 176 years, it would take less than 1 day to search a 40-bit key space. Foreign customers for U.S. products who already have DES readily available laughed at the 40-bit U.S. restriction. TIS produced a 40-bit version of Trusted Mail and obtained the expedited Department of State export approval but to date has been unable to find a foreign (or domestic) customer willing to accept the weak 40-bit key length.

After spending much energy searching for plausible solutions to this problem, our newly formed Trusted Information Systems (UK) Limited office has contracted with British scientists to implement a new UK version of PEM based on the same international specifications and using DES and RSA algorithms that are already available in the UK. In a very real sense, this situation demonstrates that the only accomplishment of U.S. export control restrictions is the export of U.S. jobs.

To make matters even worse (in the job export sense, at least), because of provisions in the UK export laws, it appears that we can *import* the UK product for sale in the U.S., something we would never be able to do in reverse.

These examples of problems with the export control process or its consequences are typical of the situations many U.S. companies find as they attempt to enter the world of software cryptography.

Industrywide Experiences

Some companies do try to compete and offer excellent DES-based products in the U.S. But because of the export restrictions, they must develop weaker versions for export if they wish to pursue foreign markets. Many companies forgo the business rather than spend extra money to develop another inferior product that cannot compete with products widely available in the market.

The Government already has a measure of lost sales and dissatisfied customers in the number of State Department/NSA export license applications denied, modified, or withdrawn. However, it is impossible to estimate accurately the full extent of lost sales. Many potential customers know that U.S. companies cannot meet their demand and thus no longer inquire. Conversely, some companies have given up even trying to get export approvals for DES to meet customer demand.

Gauging the extent of economic harm to companies is an inherently difficult task because most companies do not want to reveal that sort of information. Consequently, there exists only anecdotal information. But the accumulation of anecdotal information collected by the SPA paints a picture of three ways in which the export controls on cryptographic products are hurting American high-tech industry.

(1) First, for many data security companies, every sale is vital, and the loss of contracts smaller than $1 million can often mean the difference between life and death for these companies. The confusion and uncertainty associated with export controls on encryption generate severe problems for small firms, but not as severe as the loss of business they suffer from anti-competitive export controls. Examples abound:

- One U.S. company reported loss of revenues equal to a third of its current total revenues because export controls on DES-based encryption closed off a market when its customer, a foreign government, privatized the function for which the encryption was used, and the U.S. company was not permitted to sell to the private foreign firm. The company estimates it loses millions of dollars a year because it receives substantial orders every month from various European customers but cannot fill them because of export controls.

- One small firm could not sell to a European company because that company sold to clients other than financial institutions (for which export controls grant an exception). Later, the software firm received reports of sales of pirated copies of its software. This constituted a loss of a $400,000 contract for the small U.S. software firm.

- Because of existing export restrictions, an American company recently found itself unable to export a mass market software program that provided encryption using Canadian technology based on a Japanese algorithm. Yet other European and Japanese companies are selling competing products worldwide using the same Canadian technology.

- An SPA member's product manager in Europe reported the likely loss of at least 50% of its business among European financial institutions, defense industries, telecommunications companies, and government agencies if present restrictions on key size are not lifted.

- Yet another SPA member company reported the potential loss of a substantial portion of its international business if it cannot commit to provide DES in its programs.

- A German firm that opened a subsidiary in the U.S. sought a single source encryption software product for both its German and U.S. sites. A U.S. data security firm that bid for the contract lost the business because U.S. export controls required that the German firm would have to wait approximately six months while a license was processed to sell them software with encryption for foreign application. The license could only be for one to three years, the three year license being more expensive. Consequently, the German firm ended up purchasing a DES-based system from another German company, and the U.S. firm lost the business.

- A foreign government selected one software company's data security product as that government's security standard. The company's application to export the DES version was denied, and as a consequence the order was lost. This cost the company a $400,000 order and untold millions in future business.

(2) Second, multinational corporations (MNCs) are a prime source of business in the expanding international market for encryption products. Many U.S.-based firms have foreign subsidiaries

or operations that do not meet export requirements. While U.S. products may be competitive in the U.S., many MNCs obtain from foreign sources encryption systems that will be compatible with the company's worldwide operations. Moreover, foreign MNCs cannot rely on the availability of U.S. products and have been known to import foreign cryptography for use in their U.S. operations.

- One U.S. firm reports the loss of business from foreign MNCs that will not integrate the company's products into their U.S. operations because of the export restrictions that would prevent them from being compatible with their domestic operations.

- The Computer Business Equipment Manufacturers Association reports that one of its members was denied an export license and lost a $60 million sale of network controllers and software for encryption of financial transactions when the Western European customer could not ensure that encryption would be limited to financial transactions.

(3) Third, encryption systems are frequently sold as a component of a larger system. These "leveraged" sales offer encryption as a vital component of a broad system. Yet the encryption feature is the primary feature for determining exportability. Because of the export restrictions, U.S. firms are losing the business not just for the encryption product but for the entire system because of the restrictions on one component of it.

- One data security firm has estimated that export restrictions constrain its market opportunities by two-thirds. Despite its superior system, it has been unable to respond to requests from NATO, the Swedish PTT, and British telecommunications companies because it cannot export the encryption they demand. This has cost the company millions in foregone business.

- One major computer company lost two sales in Western Europe within the last 12 months totaling approximately $80 million because the file and data encryption in the integrated system was not exportable.

One possible solution to the problem of export controls may be for U.S. companies to relocate overseas. Some U.S. firms have considered moving their operations overseas and developing their technology there to avoid U.S. export restrictions. Thus, when a U.S. company with technology that is clearly in demand is kept from exporting that technology, it may be forced to export jobs instead.

HOW ARE U.S. CITIZENS AND BUSINESSES BEING AFFECTED BY ALL THIS?

The answer to this question is painfully simple. When U.S. industry forgoes the opportunity to produce products that integrate good security practices, such as cryptography, into their products because they cannot export those products to their overseas markets, U.S. users (individuals, companies, and Government agencies) are denied access to the basic tools they need to protect their own sensitive information. This is where the greatest frustration sets in.

The U.S. Government established export controls in order to keep good quality cryptography from proliferating outside the U.S. The result has been exactly the opposite effect. Good quality cryptography is now available everywhere in the world including the U.S. But U.S. customers cannot buy it integrated into the information system products they normally use because U.S. export laws discourage U.S. suppliers from developing such products.

We seem caught in a vicious circle that appears to make sense only to those who do not want to see good quality cryptography used anywhere.

WHAT EFFECT WILL CLIPPER HAVE?

In the midst of all of this, on April 16, 1993, the President announced the Clipper initiative to ensure the public's right to privacy while allowing law enforcement to conduct lawful wiretaps.

The principal concern of many with Clipper is the potential it has for violating the privacy of citizens. In his April 16 announcement, the President stated that "The Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law." It would appear that the only way both aspects of this policy can be carried out is if the individual's right to privacy is superseded by the Government's right to listen in whenever the Government chooses. Many people fear that this isn't much of a right to privacy.

There are many other concerns that have been expressed about the Administration's Clipper Initiative and the negative aspects of key escrow. But with respect to the issue of export restrictions on software products, Clipper represents primarily a distraction only serving to cloud the issues. Unless Clipper is made mandatory, its requirement to use hardware and its key escrow provisions will cause it to have little impact on the software market. No one will willingly give up the convenience of integrated software encryption for an expensive hardware box that will let the Government listen in.

The international aspects of Clipper are not at all thought out. Even if Clipper were exportable, the fact that the U.S. Government will hold the keys and not share them with other governments ensures that this will be no more successful overseas than the 40-bit key length "solution."

Clipper is a major diversion that does not solve any of the problems discussed above.

WHAT CAN BE DONE?

Many Calls for Action

Many people have been clamoring about the need to relax export controls on encryption for years. The National Research Council has recently issued four reports expressing serious concern in this area (Attachment 3).

The computer industry has been complaining ever more loudly for ten years.

The Congressionally chartered Computer System Security and Privacy Advisory Board has called for a national review of these issues involving Government (civilian, law enforcement, and national security interests) and industry (users and vendors). The Advisory Board passed resolutions on the need for a national review and expressing serious concerns about the Clipper Initiative (Attachment 4).

The Administration has formed an Interagency Review at the request of the President to look at all aspects of the cryptography issue including export control. This review is the highest level investigation of this problem to date. Its report is due out any time, within days or weeks. Unfortunately, the review is being conducted from behind closed doors with the only public input coming through the auspices of the Advisory Board and such industry groups as the Digital Privacy and Security Working Group.

Since the Interagency review began with the Clipper announcement and is being conducted by Government officials who are heavily committed to Clipper, it is unlikely that its results will assist business by easing the software cryptography export control constraints.

President Clinton, in commenting on the North American Free Trade Agreement, was quoted by the *Washington Post*, September 16, 1993, as saying:

> I'm telling you folks, we cannot repeal the force that is driving the world economy together. We can run away from it and get beat by it, or we can embrace it, do what we have to do and win with it.

If only those who control cryptographic exports understood this.

On September 30, the President announced a significant relaxation of the export control rules for high performance computer technology. It would be good if some of that change could affect the cryptography export area, but the present export position is so well entrenched, it is unlikely there will be much change from the Executive Branch.

The Congress Must Act Now!

The only hope for a recognition of the counterproductive nature of this situation is in the Congress. No other organization has the breadth of constituencies to allow an honest look at all the concerns and the authority to come to a definitive resolution on the issue.

We need to recognize that the U.S. public has a right to a reasonable level of protection for its sensitive information. Enabling that right through allowing the export of good quality cryptography such as DES will not harm the intelligence gathering capabilities of this country any more than the worldwide proliferation of cryptography already has.

I strongly encourage this Subcommittee to press as vigorously as possible for legislation that will allow the export of good quality cryptography so that our industry will implement it and our citizens can use it!

ATTACHMENT 1

FOREIGN TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
ASCOM Tech AG	SWITZERLAND	VINCI	HW	N
AV System Infocard	SWEDEN	??	SW/HW	N
Aarhus University	DENMARK	VICTOR	HW	N
Algorithmic Research Ltd.	ISRAEL	AR CryptoCODE	SW/HW	Y
Algorithmic Research Ltd.	ISRAEL	AR CryptoPAD	HW	Y
Algorithmic Research Ltd.	ISRAEL	AR CryptoSafe	HW	Y
Algorithmic Research Ltd.	ISRAEL	AR Crypto3270-E	SW	Y
Algorithmic Research Ltd.	ISRAEL	AR Crypto3270-P	SW/HW	Y
Algorithmic Research Ltd.	ISRAEL	AR CryptoBIOS	SW	Y
Algorithmic Research Ltd.	ISRAEL	AR CryptoCOM	SW	Y
Algorithmic Research Ltd.	ISRAEL	AR CryptoMAIN	SW	Y
Algorithmic Research Ltd.	ISRAEL	AR CryptoPC	SW	Y
Algorithmic Research Ltd.	ISRAEL	AR DISKrete	SW	Y
Antti Louko	FINLAND	AloDES	SW	Y
Ardy Elektronik AB	SWEDEN	SLD/OUS-200	HW	N
Askri	RUSSIA	Cryptos	SW	Y
British Telecom	UK	RSA chip	HW	N
CE Infosys GmbH	GERMANY	CryptCard	HW	Y
CE Infosys GmbH	GERMANY	MiniCrypt	HW	Y
CE Infosys GmbH	GERMANY	SC8810 AT Design Kit	HW	Y
CE Infosys GmbH	GERMANY	SC8820 MCA Design Kit	HW	Y
CE Infosys GmbH	GERMANY	SuperCrypt	HW	Y
CE Infosys GmbH	GERMANY	cryptLine Controller	HW	Y
CE Infosys GmbH	GERMANY	SoftCrypt	SW	Y
CNET		RSA chip	HW	N
COST Computer Security Technologies International	SWEDEN	COST-SC	SW/HW	Y
COST Computer Security Technologies International	SWEDEN	COST-Development Tools (GSL/SCL)	SW	Y
COST Computer Security Technologies International	SWEDEN	COST-EDI	SW	Y
COST Computer Security Technologies International	SWEDEN	COST-LAN	SW	Y
COST Computer Security Technologies International	SWEDEN	COST-PEM	SW	Y
Compserve Ltd	UK	Softlock 10	SW	Y
Compserve Ltd	UK	X-LOCK 10	SW	Y
Compserve Ltd	UK	X-LOCK 50	SW	Y
Concord Eracom Nederland BV	NETHERLANDS	Multi-Functional PC Security (MFPS) Card	HW	Y
Concord Eracom Nederland BV	NETHERLANDS	SECNET (FCM)	SW/HW	Y
Concord Eracom Nederland BV	NETHERLANDS	SECNET (HCM)	HW	Y
Concord Eracom Nederland BV	NETHERLANDS	SECNET FBI-Encryptor	HW	Y
Concord Eracom Nederland BV	NETHERLANDS	SECNET MFPS	SW/HW	Y
Concord Eracom Nederland BV	NETHERLANDS	DEA Crypto Toolkit	SW	Y

FOREIGN TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Concord Eracom Nederland BV	NETHERLANDS	SCORE	SW	Y
Concord Eracom Nederland BV	NETHERLANDS	SECNET (SCM)	SW	Y
Cryptech NV/SA	BELGIUM	DES-CHIP	HW	Y
Cryptech NV/SA	BELGIUM	PC-Crypto Toolkit	HW	Y
Cryptech NV/SA	BELGIUM	PC-RSA Processor	HW	N
Cryptech NV/SA	BELGIUM	RSA Processor	HW	N
Cryptech NV/SA	BELGIUM	DES Software Toolkit	SW	Y
CryptoMathic	DENMARK	Multiprecision Kernel	HW	N
CryptoMathic	DENMARK	DES Kernel	SW	Y
CryptoMathic	DENMARK	DES Security Mechanisms	SW	Y
CryptoMathic	DENMARK	F2F (File-to-File)	SW	Y
CryptoMathic	DENMARK	RSA Security Mechanisms	SW	N
Cryptomathic	DENMARK	6303 SIS	SW	N
Cryptomathic	DENMARK	8051 DES	SW	Y
Cryptomathic	DENMARK	DSP 56000 DES	SW	Y
Cryptomathic	DENMARK	DSP 56000 RSA	SW	N
Cryptomathic	DENMARK	PIC16C57 SIS	SW	N
Cryptomathic	DENMARK	FRAS-File RSA	SW	N
Cybanim Pty Ltd.	AUSTRALIA	DES32 v1.02	SW	Y
Cybanim Pty Ltd.	AUSTRALIA	LUC 2.03	SW	N
Cybanim Pty Ltd.	AUSTRALIA	RSAz 1.20	SW	N
DEC		RSA chip	HW	N
Data Innovation Ltd.	UK	ED500	HW	Y
Data Innovation Ltd.	UK	ED600	HW	N
Data Innovation Ltd.	UK	ED600R	HW	N
Data Innovation Ltd.	UK	Network Security Workstation (NSW)	SW/HW	Y
Data Safe	GERMANY	WINDEX	SW	N
DataSoft International Ltd.	UK	DataCode	SW	N
DataSoft International Ltd.	UK	DataTalk	SW	N
Dynatech Communications Ltd.	UK	Cipher 2200	HW	N
Dynatech Communications Ltd.	UK	Cryptopad	HW	Y
Dynatech Communications Ltd.	UK	Cybercrypt LE	HW	Y
Dynatech Communications Ltd.	UK	Multicrypt	HW	Y
Elias Ltd.	RUSSIA	Excellence for DOS	SW	N
Eracom Pty Ltd.	AUSTRALIA	ERA 2007 Line Encryptor	HW	Y
Eracom Pty Ltd.	AUSTRALIA	ERA 4007 Line Encryptor	HW	Y
Eracom Pty Ltd.	AUSTRALIA	Eracom Security Module (ESM)	HW	Y
Eracom Pty Ltd.	AUSTRALIA	Micro Channel Slave Encryptor (MCSE-16)	HW	Y
Eracom Pty Ltd.	AUSTRALIA	Micro Channel Slave Encryptor (MCSE-8)	HW	Y

FOREIGN TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Eracom Pty Ltd.	AUSTRALIA	PC Encryptor (PCE-16)	HW	Y
Eracom Pty Ltd.	AUSTRALIA	PC Encryptor (PCE-8)	HW	Y
Eracom Pty Ltd.	AUSTRALIA	ProtectSNA	SW/HW	Y
Eracom Pty Ltd.	AUSTRALIA	Secure Access System Software (SAS)	SW	Y
Eracom Pty Ltd.	AUSTRALIA	Windows Application Security Program (WASP)	SW	Y
Eric Young	AUSTRALIA	fcrypt	SW	Y
Eric Young	AUSTRALIA	libdes	SW	Y
Eurologic Systems	IRELAND	Datacrypt	HW	N
GEC-Marconi Secure Systems	UK	DATALOK H	HW	N
GEC-Marconi Secure Systems	UK	DATALOK L	HW	N
GEC-Marconi Secure Systems	UK	MASC Crypto Management System	SW	N
GEC-Marconi Secure Systems	UK	Marcrypt	HW	N
GMD	GERMANY	SecuDE-4.1	SW	N
GN Datacom	DENMARK	safeMatic Security Module	HW	Y
Global CIS Ltd	UK	Safeguard Security System	SW	N
Greta AG	SWITZERLAND	Gretacoder 545	HW	Y
Gretag AG	SWITZERLAND	Gretacoder 522	HW	Y
Gretag AG	SWITZERLAND	Gretacoder 524	HW	Y
Gretag AG	SWITZERLAND	Gretacoder 526	HW	Y
Gretag AG	SWITZERLAND	Gretacoder 605	HW	Y
Highware, Inc.	BELGIUM	Fileguard		N
Incaa Datacom BV	NETHERLANDS	AUTHORIZER	HW	N
Info Guard AG	SWITZERLAND	I-1100	HW	Y
Info Guard AG	SWITZERLAND	I-1200	SW/HW	Y
Info Guard AG	SWITZERLAND	I-2010	HW	Y
Info Guard AG	SWITZERLAND	I-3010	HW	N
Info Security Systems	UK	SecureInfo	HW	N
InfoGuard AG	SWITZERLAND	I-1200 DES Software	SW	Y
Isolation Systems	CANADA	ISAC 1100	SW/HW	Y
Isolation Systems	CANADA	ISAC 1500	SW/HW	Y
Isolation Systems	CANADA	ISAC 2200	HW	Y
Isolation Systems	CANADA	ISAC 2400	HW	Y
Isolation Systems	CANADA	ISAC 2500	HW	Y
Isolation Systems	CANADA	ISAC 3200	HW	Y
Isolation Systems	CANADA	ISAC 3500	HW	Y
Isolation Systems	CANADA	ISAC 4200	HW	Y
Isolation Systems	CANADA	ISE 2100	HW	Y
J.R. Ward Computes Ltd.	UK	Code-It	SW	N
JPY Associated, Ltd.	UK	DataLock Editor(DLE)	SW	Y

FOREIGN TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
JPY Associates	UK	DataLock, Version 3.1	SW	Y
JPY Associates, Ltd.	UK	DataLock CIPHER Procedura	SW	Y
Jaguar Communications Ltd.	UK	ZCODA-A	HW	N
Jaguar Communications Ltd.	UK	ZCODA-X	HW	N
LAN Crypto	RUSSIA	ATHENA	SW	N
LAN Crypto	RUSSIA	VESTA-1	SW	Y
LAN Crypto	RUSSIA	VESTA-2	SW	Y
LSI Logic/Dataco AS	DENMARK	DATACO LSA4043 2030025402	HW	Y
Microft Technology Inc.	UK	CLAM	SW	N
Micronyx UK Ltd.	UK	Trispan	SW	N
Micronyx UK Ltd.	UK	Triumph V2	SW	Y
Newbridge Microsystems	CANADA	CA20C03A	HW	Y
Newnet S.A.	ARGENTINA	DSD 9612 Data Security Device	HW	Y
News Datacom	AUSTRALIA	N-Sure Access 1000	HW	Y
Northern Telecom Canada Limited	CANADA	Packet Data Security Overlay (PDSO)	HW	Y
Okiok Data	CANADA	Data Encryption Board (DEB)	HW	Y
Okiok Data	CANADA	RAC/M 3.0	SW/HW	Y
Okiok Data	CANADA	RAC/M II 3.0	SW/HW	Y
Okiok Data	CANADA	FAS-PACK	SW	Y
Omnisec AG	SWITZERLAND	Omnisec 810	HW	N
Omnisec AG	SWITZERLAND	Omnisec 820	HW	N
Omnisec AG	SWITZERLAND	Omnisec 830	HW	N
Omnisec AG	SWITZERLAND	Omnisec 840	HW	N
PC Security Ltd	UK	CP8-AuthentICC	HW	N
PC Security Ltd	UK	LapGUARD	SW	N
PC Security Ltd.	UK	Stoplock III	SW	N
PC Security Ltd.	UK	Stoplock IV	SW	Y
Peter Gutmann	NEW ZEALAND	HPACK Archiver	SW	N
Philips Communication Systems	FRANCE	P83C852 Smart Card Crypto Controller	HW	N
Plessey Crypto	UK	RSA chip	HW	N
Plus 5 Engineering Ltd	UK	Policeman	SW	N
Protection Systems Ltd.	UK	Guardian Angel Plus	SW	Y
Queen's University		RSA chip	HW	N
Racal-Milgo	UK	Datacrptor Key Management Center	HW	N
S&S International	UK	SAVEDIR	SW	N
SONOR International AB	SWEDEN	HR&S	SW	N
ScanTech	RUSSIA	Krypton	HW	N
Secured Communication International Ltd.	CANADA	PCMCIA	HW	Y
SecuriCrypto AB	SWEDEN	SecuriCrypto V.24	HW	N

FOREIGN TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
SecuriCrypto AB	SWEDEN	SecuriCrypto V.248	HW	N
SecuriCrypto AB	SWEDEN	SecuriCrypto V.35	HW	N
SecuriCrypto AB	SWEDEN	SecuriCrypto V.36	HW	N
SecuriCrypto AB	SWEDEN	SecuriCrypto X.21	HW	N
SecuriCrypto AB	SWEDEN	SecuriCrypto X.25	HW	N
SecuriCrypto AB	SWEDEN	SecuriCrypto X.26	HW	N
Shareware plc	UK		SW	Y
Shareware plc	UK	DES	SW	Y
Shareware plc	UK	PC-IRIS	SW	Y
Shareware plc	UK	PC-Merlin	SW	Y
Smart Diskette	FRANCE	Very Smart Disk	HW	Y
Sophos Ltd.	UK	CRYPTO-JET	HW	Y
Sophos Ltd.	UK	DES Toolkit	SW	Y
Sophos Ltd.	UK	EDS	SW	Y
Sophos Ltd.	UK	PUBLIC	SW	Y
Sophos Ltd.	UK	RSA Toolkit	SW	N
Stig Ostholm	SWEDEN	DES Implementation 2.0	SW	Y
TELECRYPT, Ltd.	RUSSIA	TELECRYPT	SW	Y
Technetics	SOUTH AFRICA	N3000M		N
Tele Security Timmann Gm&H & Co.	GERMANY	TST 3010 High Performance Mil-Spec Cipher Terminal	HW	N
Tele Security Timmann Gm&H & Co.	GERMANY	TST 3550 Handy Crypt	HW	N
Tele Security Timmann Gm&H & Co.	GERMANY	TST 3570 Pocketcrypt	HW	N
Tele Security Timmann Gm&H & Co.	GERMANY	TST 3677 VDU/Screen-Oriented Headquarter Cipher	HW	N
Tele Security Timmann Gm&H & Co.	GERMANY	TST 5560 DataCipher Set	HW	N
Tele Security Timmann Gm&H & Co.	GERMANY	TST 9669 Telex Cipher Module	HW	N
Tele Security Timmann GmbH & Co.	GERMANY	TST 5573 C	HW	N
Tele Security Timmann GmbH & Co.	GERMANY	TST 5573 H/C	HW	N
Tele Security Timmenn GmbH & Co.	GERMANY	TST 5573 PC	HW	N
Tele Security Timmann GmbH & Co.	GERMANY	TST 5573 X/C	HW	N
The Software Forge Ltd.	UK	Data Jumbler	SW	Y
Triple D Ltd.	HONG KONG	P-8 Security Master Card	SW/HW	Y
UTI-MACO GmbH	GERMANY	SAFE-Board I	HW	N
UTI-MACO GmbH	GERMANY	SAFE-Board II	HW	Y
UTI-MACO GmbH	GERMANY	SAFE-Board III	HW	Y
UTI-MACO GmbH	GERMANY	BACK-Guard	SW	Y
UTI-MACO GmbH	GERMANY	C:Crypt	SW	Y
UTI-MACO GmbH	GERMANY	SAFE-Guard EZ	SW	Y
UTI-MACO GmbH	GERMANY	SAFE-Guard OS/2 3.0	SW	Y
UTI-MACO GmbH	GERMANY	SAFE-Guard Professional 3.2C	SW	Y

FOREIGN TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
UTI-MACO GmbH	GERMANY	SIGN-Guard	SW	Y
University College London	UK	OSISEC	SW	Y
University College London	UK	UK DRA-PEM	SW	Y
Verspeck & Soeters b.v.	NETHERLANDS	SecuriO	HW	Y
Verspeck & Soeters b.v.	NETHERLANDS	SecuriO I	HW	Y
Verspeck & Soeters b.v.	NETHERLANDS	SecuriO II	HW	N
Verspeck & Soeters b.v.	NETHERLANDS	SecuriO III	HW	Y
Zeta Communications Ltd.	UK	Zetacoda A	HW	N
Zeta Communications Ltd.	UK	Zetacoda X	HW	N

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
AO Electronics	USA	X-Lock-100	SW/HW	N
AO Electronics	USA	X-Lock-50	SW/HW	Y
ASC Systems	USA	Communications Encryption Controller	HW	Y
ASC Systems	USA	DES/COMM	HW	N
ASD Software Inc.	USA	Fileguard	SW	N
AT&T	USA	AT&T Secure Data Device, Model 1900	HW	N
AT&T	USA	STU-III Secure Data Device Model 1910	HW	N
AT&T Datotek	USA	DKT-1000	HW	N
AT&T Datotek	USA	DLE-7000 Synchronous DataLink Encryptor	HW	N
AT&T Datotek	USA	DPC-3000 MicroCryptor	HW	N
AT&T Datotek	USA	XMP-800 Ciphering Message Processor	HW	N
Advanced Encryption Systems	USA	Network Security System	HW	Y
American Computer Security	USA	EasyLock	SW	Y
Apple Computer	USA	PowerTalk	SW	N
Applied Software	USA	Data Encryption Facility (DEF)	SW	Y
Ashton Tate	USA	dBase IV		N
BCC	USA	DES-AT	HW	Y
BCC	USA	SL007 Personal Secure Notebook Computer	HW	Y
BLOC Development Corporation	USA	F3 Fill (with Security)	SW	N
Banyan	USA	Vines		N
Bi-Hex	USA	Cryptex	SW	N
Borland	USA	Paradox		N
Casady and Greene	USA	AME (Access Managed Environment) 1.1.3	SW	Y
Centel Federal Systems	USA	Net/Assure	SW/HW	Y
Centel Federal Systems	USA	Net/Assure Server	SW/HW	Y
Centel Federal Systems	USA	PC/Assure 3.4	SW/HW	Y
Central Point Software	USA	PC Tools Deluxe		N
Certus International	USA	Certus	SW	N
Cettlan Corp.	USA	SecureModem 2032e	HW	Y
Clarion	USA	Clarion Professional Development		N
Codex	USA	??		N
Command SW Systems	USA	FREEZE 4.0	SW	Y
Command SW Systems	USA	FREEZE PLUS 4.0	SW	Y
Command SW Systems	USA	LANGUARD	SW	Y
Command SW Systems	USA	Security Guardian	SW	Y
Commcrypt	USA	ACCESSGuard	SW	N
Commcrypt	USA	CryptoLock	SW	Y
Communication Devices Inc.	USA	Remote Encryptor	HW	Y
Complan	USA	DESQIK	SW	Y

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Computer Associates International, Inc.	USA	CA-ACF2/PC 1.0	SW	Y
Computer Associates International, Inc.	USA	CA-CORTANA 1.0	SW	Y
Computer Associates International, Inc.	USA	CA-Top Secret/PC 1.0	SW	Y
Contemporary Cybernetics	USA	CY-2000	HW	N
Cryptall	USA	DPU-1000	HW	Y
Cryptall	USA	DPU-1000S	HW	Y
Cryptall	USA	DPU-1000X	HW	Y
Cryptech	USA	Redoc-Cuts	HW	N
Cylink Corp.	USA	Advanced Smart Card	HW	N
Cylink Corp.	USA	CIDEC-HS	HW	Y
Cylink Corp.	USA	CIDEC-HX	HW	N
Cylink Corp.	USA	CIDEC-LS	HW	Y
Cylink Corp.	USA	CIDEC-LX	HW	N
Cylink Corp.	USA	CIDEC-MLX Central Encryption System	HW	N
Cylink Corp.	USA	CIDEC-MS	HW	Y
Cylink Corp.	USA	CIDEC-VH	HW	N
Cylink Corp.	USA	CIDEC-VHS	HW	Y
Cylink Corp.	USA	CKG-VHS Data Encryptor	HW	N
Cylink Corp.	USA	CY512	HW	N
Cylink Corp.	USA	LS-20 Low-Speed Data Encryptor	HW	N
Cylink Corp.	USA	LS-20 Low-Speed Data Encryptor	HW	Y
Cylink Corp.	USA	SecurePC	SW/HW	Y
Cylink Corp.	USA	SecurePC/T	SW/HW	Y
Cylink Corp.	USA	VY 1024	HW	N
DSC Communications	USA	Nexos		N
DataEase International	USA	DataEase		N
DataMedia Corporation	USA	SECUREcard Model 200	SW	Y
DataMedia Corporation	USA	SECUREcard Model 400		Y
Datamedia Corporation	USA	SECUREcard Model 100	HW	Y
Datamedia Corporation	USA	SECUREchange	SW	Y
Datotek, Inc.	USA	D.U.D.E.	HW	Y
Digital Enterprises	USA	Deadbolt	HW	Y
Digital Enterprises	USA	Netlock	HW	N
Digital Enterprises	USA	Propack	HW	N
Digital Enterprises	USA	Shockpack	HW	N
Digital Equipment Corp	USA	VAX Encryption	SW	Y
Digital Pathways	USA	Defender II	HW	Y
Digital Pathways	USA	SecureNet Key		N
ELIASHIM Microcomputers Inc	USA	CodeSafe	SW	N

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
EMUCOM	USA	??		N
Enigma Logic, Inc.	USA	SafeWord PC-Safe II	SW	Y
Enigma Logic, Inc.	USA	SafeWord PC-Safe III	SW	Y
Eracom Pty Ltd.	USA	Series 90 ESM	HW	Y
Fifth Generation Systems	USA	DiskLock	SW	Y
Fifth Generation Systems	USA	DiskLock PC	SW	Y
Fischer International	USA	Watchdog Armor	SW/HW	Y
Fischer International	USA	Kryptonite	SW	Y
Fischer International	USA	MailSafe	SW	N
Fischer International	USA	RSA/3270	SW	Y
Fischer International	USA	SafeBoot	SW	N
Fischer International	USA	Watchdog Director	SW	N
Fischer International	USA	Watchdog PC Data Security 6.0	SW	Y
Glenco Engineering	USA	GLEN-DES	HW	Y
Glenco Engineering	USA	Hardlock 1.01	HW	N
Glenco Engineering	USA	Hardlock-DES	HW	N
Glenco Engineering	USA	HL-Crypt	SW	N
Hawkeye Gralix, Inc.	USA	DES-PAC 3.0	SW	Y
Hughes Data Systems Inc.	USA	SECUREPC	SW	N
Hughes Data Systems Inc.	USA	SECUREPC PLUS	SW	N
Hybrid Communications	USA	CE Infosys boards for S-bus		N
IBM	USA	IBM 4754 Security Interface Unit	HW	Y
IBM	USA	IBM 4755 Cryptographic Adapter Card	HW	Y
IBM	USA	IBM Integrated Cryptographic Feature (ICRF)	HW	Y
INFOSAFE	USA	X-Lock 10		N
INFOSAFE	USA	X-Soft 10		N
Information Conversion Services	USA	CRYPTMASTER		N
Information Security Corp.	USA	Crypt Master 3.10	SW	Y
Information Security Corp.	USA	Secret Agent	SW	Y
Information Security Corp.	USA	SpyProof	SW	Y
Isolation Systems, Inc.	USA	ISAC 2300	HW	Y
Jones Futurex, Inc.	USA	ENC-300A	HW	Y
Jones Futurex, Inc.	USA	ENC-324	HW	Y
Jones Futurex, Inc.	USA	ENC-326	HW	Y
Jones Futurex, Inc.	USA	ENC-334	HW	Y
Jones Futurex, Inc.	USA	ENC-336	HW	Y
Jones Futurex, Inc.	USA	ENC-526	HW	Y
Jones Futurex, Inc.	USA	Protec Plus	SW/HW	N
Kensington Microware Ltd.	USA	Passproof	SW/HW	Y

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Kent Marsh Ltd.	USA	MacSafe II 2.0	SW	Y
Key Concepts	USA	SureKey/2	SW	N
Kinetic Corp.	USA	Kinetic Encryption 2.0	SW	Y
Lassen Software, Inc.	USA	Trusted Access	SW	N
Lattice Inc.	USA	SecretDisk II	SW	Y
Lemcom Systems	USA	DigiSig plus DES	HW	Y
Lemcom Systems	USA	ViaCrypt	HW	Y
Litronic	USA	Lead/Argus		N
Litronic Industries (Information Systems Div.)	USA	ARGUS	HW	Y
Litronic Industries (Information Systems Div.)	USA	LEAD	HW	N
Lotus	USA	Lotus Notes	SW	N
Lotus	USA	Lotus 123		N
Lotus	USA	cc:Mail		N
MCTel	USA	MCTel Security System	SW	Y
Maedae Enterprises	USA	Encrypt-It v2.0	SW	Y
Magna	USA	Empower I 4.0	SW	Y
Magna	USA	Empower II 4.0	SW	Y
Magna	USA	Empower III 4.0	SW	Y
Massachusetts Institute of Technology(MIT)	USA	Techmail with PEM	SW	Y
Mergent International	USA	PC/DACS 20201	SW	Y
Mergent International	USA	SSO/DACS	SW	Y
Micanopy MicroSystems Inc.	USA	ZCrypt 1.2	SW	N
Micro Security Systems Inc.	USA	SECURIDATA	HW	N
Micro Securiyt Systems Inc.	USA	DecuriKey	HW	Y
MicroFrame Inc.	USA	CipherKEY	HW	Y
MicroFrame Inc.	USA	DataLOCK 4000	HW	Y
MicroFrame Inc.	USA	Dataguard 4000	HW	Y
Microcom Inc. (Utilities Product Group)	USA	Citadel	HW	Y
Micronyx	USA	TRISPAN	SW/HW	N
Micronyx	USA	SAFE	SW	N
Micronyx	USA	Secured DOS	SW	N
Micronyx	USA	Triumph!	SW	Y
Microrim	USA	R:Base		N
Microsoft	USA	Excel		N
Microsoft	USA	LAN Manager 2.0		N
Microsoft	USA	Mail 2.x		N
Microsoft	USA	Mail 3.0 for MAC		N
Microsoft	USA	Word 2.0 for Windows		N
Motorola	USA	Network Encryption Systems (NES)		N

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Norton	USA	Norton Utilities 4.0+		N
Novell	USA	NameService		N
Novell	USA	Netware 386 3.1		N
PC Dynamics Inc.	USA	Total Security	SW	Y
PC Guardian	USA	DES Encryption	SW	Y
PC Guardian	USA	Data Security Plus	SW	Y
PC Plus Inc.	USA	Ultron SSP3110 Data Storage Encryptor	HW	N
Paradyne Corporation	USA	InfoLock 1027 Model 2811-03	HW	Y
Paradyne Corporation	USA	InfoLock Model 2811-11	HW	Y
Personal Computer Card Corp.	USA	LepGuard	SW	Y
Personal Computer Card Corp.	USA	PCSS	SW	Y
Prime Factors	USA	DESCRYPT & DESCRYPT+	SW	Y
Prime Factors	USA	DESCRYPT/BS & DESCCRYPT+/BS	SW	Y
Prime Factors	USA	DESCRYPT/C & DESCRYPT+/C	SW	Y
Prime Factors	USA	DESCRYPT/CS & DESCRYPT+/CS	SW	Y
Prime Factors	USA	DESCRYPT/FS & DESCRYPT+/FS	SW	Y
Prime Factors	USA	DESCRYPT/MS	SW	Y
Prime Factors	USA	Diogenes	SW	Y
Prime Factors	USA	PIN Management System	SW	Y
Prime Factors	USA	PINSYS & PINSYS+	SW	Y
Prime Factors	USA	PSYPHER & PSYPHER+	SW	Y
Prime Factors	USA	PSYPHER/VM	SW	Y
Prime Factors	USA	PSYPHER/VS	SW	Y
Prime Factors	USA	u-PSYPHER	SW	Y
RSA Data Security	USA	RSA/DSP	HW	Y
RSA Data Security	USA	BSAFE 2.0	SW	Y
RSA Data Security	USA	MailSafe 5.0	SW	Y
RSA Data Security	USA	TIPEM	SW	Y
RSA Laboratories	USA	RSAREF	SW	Y
Racal-Datacom	USA	Datacryptor 64	HW	Y
Racal-Datacom	USA	Datacryptor 64-1027	HW	Y
Racal-Guardata	USA	Asynchronous Gateway	HW	Y
Racal-Guardata	USA	CAT-2000, 2001, 2001H	HW	Y
Racal-Guardata	USA	CAT-2080	HW	Y
Racal-Guardata	USA	Gateway Security	HW?	Y
Racal-Guardata	USA	Host Security Module (HCM)	HW	Y
Racal-Guardata	USA	ISM-444	HW	Y
Racal-Guardata	USA	Personal Computer Security Module (PCSM)	HW	Y
Racal-Guardata	USA	X26 Gateway	HW	Y

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS
AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Racal-Guardata	USA	X9 Cryptoserver	HW	Y
Rainbow Technology	USA	DataSentry	HW	Y
Raxco	USA	DataLock	SW	N
SCO	USA	SCO Unix System V/386		N
Safetynet	USA	StopLight	SW	Y
Samna Corp.	USA	Ami Pro		N
Sector Technology	USA	Sentinel 4.04	HW	Y
Sector Technology	USA	Citadel 4.04	SW	Y
Sector Technology	USA	Port of Entry 2.0	SW	Y
Secura Technologies	USA	LAPSECURE	HW	N
Security Microsystems Inc.	USA	DesMaster Hardware 1.0	HW	Y
Security Microsystems Inc.	USA	Lockit I Extended Edition 3.0	HW	Y
Security Microsystems Inc.	USA	LockIt Professional 2.14	SW/HW	Y
Security Microsystems Inc.	USA	DesMaster Software	SW	Y
Security Microsystems Inc.	USA	Lockit III 2.03	SW	N
Sentry Systems, Inc.	USA	STOPLOCK IV	SW/HW	Y
Software Directions, Inc.	USA	Softsafe 2.0	SW	N
Solid Oak Software	USA	PC-Sentry	SW	N
SophCo, Inc.	USA	PROTEC 3.5A	SW	Y
Sola Miltope	USA	PassPort Communications Security System		Y
Sterling Software Inc. (Sys. SW Mktg. Div.)	USA	Shrink	SW	N
Symantec	USA	Q&A 4.0		N
Techmar Computer Products, Inc.	USA	COMLOCK	SW	N
Techmar Computer Products, Inc.	USA	IRICRYPT	SW	N
Techmatics	USA	CEInfosys CryptCard		N
Techmatics, Inc.	USA	CryptCard	SW/HW	Y
Thumbscan, Inc.	USA	PCBoot 2.50	HW	N
Thumbscan, Inc.	USA	SoftBoot 2.50	SW	N
Trigram Systems	USA	DES Module	SW	Y
Trigram Systems	USA	DataSafe	SW	Y
Trusted Information Systems, Inc.	USA	Trusted Mail	SW	Y
Trusted Information Systmes, Inc.	USA	TIS/PEM	SW	Y
UUNet Technologies, Inc.	USA	Lan Guardian		N
United Software Security	USA	Privacy Plus 3.01	SW	Y
VLSI	USA	VM007 Encryption Processor	HW	Y
Verdix Corp. (Secure Product Division)	USA	VSLAN	HW	Y
Visionary Electronics	USA	Visionary 2400XT	HW	N
Wang Laboratories	USA	Trusted Interface	HW	N
Wang Labs	USA	TIU		N

DOMESTIC TEXT, FILE, DATA ENCRYPTION PROGRAMS AND PRODUCTS IDENTIFIED BY THE SPA (as of October 9, 1993)

Company Name	Country	Product Name	SW/HW	DES
Westerm DataCom Co. Inc.	USA	MESA 432, 432I	HW	Y
WordPerfect	USA	WordPerfect		N
WordPerfect	USA	WordPerfect Office		N
XTree	USA	XTree Net 2.0		N
hDC	USA	hDC FileApps		N
usrEZ Software, Inc.	USA	Camouflage	SW	N
usrEZ Software, Inc.	USA	ultraSHIELD	SW	N

ATTACHMENT 2

COMPANIES MANUFACTURING AND/OR DISTRIBUTING CRYPTOGRAPHIC PRODUCTS WORLDWIDE

From the Software Publishers Association survey of cryptographic products as of October 12, 1993.

ARGENTINA	Newnet S.A.
AUSTRALIA	Cybanim Pty Ltd.
	Datamatic Pty Ltd.
	Eric Young
	Loadplan Australasia Pty Ltd.
	News Datacom
	RANDATA Pty Ltd.
	Robust Software
	Ross Williams
	Sagem Australasia Pty Ltd.
	TRAC Systems
	Tracom
AUSTRIA	Schrack-Dat
BAHRAIN	International Information Systems
BELGIUM	Cryptech NV/SA
	GSA Ran Data Europe
	Highware, Inc.
	Unina SA
	Vector
CANADA	A.B. Data Sales, Inc.
	Concord-Eracom Computer Ltd.
	Isolation Systems
	Mobius Encryption Technologies
	Newbridge Microsystems
	Northern Telecom Canada Limited
	Okiok Data
	Paradyne Canada Ltd.
	Secured Communication Internation

DENMARK	Aarhus University
	CryptoMathic
	GN Datacom
	Iversen & Martens A/S
	LSI Logic/Dataco AS
	Swanholm Computing A/S
FINLAND	Antti Louko
	Ascom Fintel OY
	Instrumentoiti OY
FRANCE	CCETT
	CSIL
	Cryptech France
	Digital Equipment Corporation (DEC)
	Incaa France S.A.R.L.
	LAAS
	Philips Communication Systems
	Rast Electronics
	S.A. Gretag
	Smart Diskette
	Societe Sagem
GERMANY	AR Datensicherungssysteme GmbH
	CE Infosys GmbH
	Concord-Eracom Computer GmbH
	Controlware GmbH
	Data Safe
	Dynatech-Gesellschaft fur Datenve
	GMD
	Gretag Elektronik GmbH
	KryptoKom
	Markt & Technik Software Partners
	Paradyne GmbH
	Siemens
	Smart Diskette GmbH
	Tela Versicherung
	Tele Security Timmann
	Telenet Kommunication
	The Compatibility Box GmbH
	Tulip Computers
	UTI-MACO GmbH

GREECE	G.J.Messaritis & Co. Ltd.
	ORCO Ltd.
HONG KONG	News Datacom
	Triple D Ltd.
INDIA	Chenab Info Technology
IRELAND	Eurologic Systems
	Renaissance Contingency Services
ISRAEL	Algorithmic Research Ltd.
	ELYASIM
	News Datacom
	TADIRAN
ITALY	Incaa SRL
	Ratio Srl
	Telvox s.a.s.
	Uniautomation
JAPAN	Fujitsu BSE
	Japan's National Defense Academy
	Paradyne Japan, KK
	Yokohama National University
LUXEMBORG	Telindus SA
MALTA	Shireburn Co. Ltd.
NETHERLANDS	CRYPSYS Data Security
	Concord Eracom Nederland BV
	Cryptech Nederland
	DSP International
	David Chaum
	Geveke Electronics BV
	Incaa Datacom BV
	Incaa Nederland BV
	Repko BV Datacomms
	Verspeck & Soeters BV
NEW ZEALAND	Peter Gutmann
	Peter Smith and Michael Lennon

NORWAY	BDC Bergen Data Consulting A/S Scand PC Sys/Sectra Skanditek A/S UMI SA
PORTUGAL	Infornova Redislogar SA
RUSSIA	Askri Elias Ltd. LAN Crypto RESCrypto ScanTech TELECRYPT, Ltd.
SAUDI ARABIA	Info Guard Saudi Arabia
SINGAPORE	Communications Systems Engineering Digitus Computer Systems
SOUTH AFRICA	BSS (Pty) Ltd. Computer Security Associates EFT Intelligent Nanoteq Net One Spescom Technetics
SPAIN	Redislogar Comminicaciones SA Sinutec Tecnitrade Int. SA
SWEDEN	AV System Infocard Ardy Elektronik AB Au-System Infocard AB COST Computer Security Technologies QA Informatik AB SONOR International AB SecuriCrypto AB Stig Ostholm Tomas Tesch AB

SWITZERLAND	ASCOM Tech AG
	Brown-Boveri
	Crypto AG
	ETH Zurich
	Ete-Hager AG
	Gretag AG
	Incaa Datacom AG
	Info Guard AG
	Omnisec AG
	Organa
UK	Airtech
	British Telecom
	Business Simulations
	Cambridge Electric Industries
	Codepoint Systems Ltd.
	Compserve Ltd.
	Computer Associates
	Computer Security Ltd.
	Cylink Ltd.
	Data Innovation Ltd.
	DataSoft International Ltd.
	Datamedia Corporation, Ltd.
	Dynatech Communcations Ltd.-North
	Dynatech Communication Ltd.
	Engrus
	Fulcrum Communications
	GEC-Marconi Secure Systems
	Gelosia
	Global CIS Ltd.
	Gretag Ltd.
	Honeywell
	IT Security International
	ITV
	Incaa UK
	Interconnections
	International Data Security
	International Software Management
	J.R.Ward Computers Ltd.
	JPY Associates
	Jaguar Communications Ltd.
	Janus Sovereign
	Loadplan
	Logica

UK	Marconi
	Microft Technology Inc.
	Micronyx UK Ltd.
	Network Systems
	News Datacom
	Northern Telecom Europe Limited
	PC Security Ltd.
	Paradyne European Headquarters
	Plessy Crypto
	Plus 5 Engineering Ltd.
	Prosoft Ltd.
	Protection Systems Ltd.
	Racal
	Racal Milgo
	Radius
	S&S International
	Shareware plc
	Sington Associates
	Smart Diskette UK
	Smith's Associates
	Softdiskette
	Sophos Ltd.
	Stralfors Data
	Sygnus Data Communications
	The Software Forge Ltd.
	Time & Data Systems
	Tricom
	University College London
	Widney Ash
	Zergo
	Zeta Communications Ltd.
USA	AO Electronics
	AOS
	ASC Systems
	ASD Software Inc.
	ASP
	AT&T
	AT&T Datotek Inc.
	Access Data Recovery
	Advanced Computer Security Concepts
	Advanced Encryption Systems
	Advanced Information Systems
	American Computer Security

USA	Applied Software Inc.
	Ashton Tate
	BCC
	BLOC Development Corporation
	Banyan
	Bi-Hex Co.
	Borland
	Braintree Technology
	CE Infosys of America, Inc.
	Casady and Greene
	Centel Federal Systems Inc.
	Central Point Software
	Certus International
	Clarion
	Codex
	Command SW Systems
	Commcrypt
	Communication Devices Inc.
	Complan
	Computer Associates International
	Contemporary Cybernetics
	Cryptall
	Cryptech
	Cryptex/Gretag Ltd.
	Cylink
	Cypher Comms Technology
	DSC Communications
	DataEase International
	Datamedia Corp. (DC Area)
	Datamedia Corporation
	Datotek, Inc.
	Digital Enterprises Inc.
	Digital Equipment Corporation (DEC)
	Digital Pathways
	Dolphin Software
	Dowty Network Systems
	ELIASHIM Microcomputers Inc.
	EMUCOM
	Enigma Logic, Inc.
	Fifth Generation Systems, Inc.
	Fischer International
	GN Telematic Inc.
	Glenco Engineering
	Hawk Technologies Inc.

USA	Hawkeye Grafix, Inc.
	Hughes Data Systems Inc.
	Hughes Network Systems - California
	Hughes Network Systems - Maryland
	Hybrid Communications
	International Business Machines (IBM)
	INFOSAFE
	Incaa Inc.
	Info Resource Engineering
	Info Security Systems
	Information Conversion Sevices
	Information Security Corp.
	Isolation Systems, Inc.
	Jones Futurex, Inc.
	Kensington Microware Ltd.
	Kent Marsh Ltd.
	Key Concepts
	Kinetic Corp.
	Lassen Software, Inc.
	Lattice Inc.
	Lemcom Systems
	Litronic Industries
	Lotus
	MCTel
	Maedae Enterprises
	Magna
	Massachusetts Institute of Technology
	Mergent International
	Micanopy MicroSystems Inc.
	Micro Security Systems Inc.
	MicroFrame Inc.
	MicroLink Technologies Inc.
	Microcom Inc. (Utilities Product Group)
	Micronyx
	Microrim
	Microsoft
	Mika, L.P.
	Motorola
	Networking Dynamics Corp.
	Northern Telecom Inc.
	Norton
	Novell
	OnLine SW International
	Ontrak Computer Systems Inc.

USA	Otocom Systems Inc.
	Paradyne Caribbean, Inc.
	PC Access Control Inc.
	PC Dynamics Inc.
	PC Guardian
	PC Plus Inc.
	Paradyne Corporation
	Personal Computer Card Corp.
	Prime Factors
	RSA Data Security, Inc.
	RSA Laboratories
	Racal-Datacom
	Racal-Guardata
	Rainbow Technology
	Raxco
	S Squared Electronics
	SCO
	SVC
	Safetynet
	Samna Corp
	Sector Technology
	Secura Technologies
	Security Microsystems Inc.
	Semaphore Communications
	Sentry Systems, Inc.
	Software Directions, Inc.
	Solid Oak Software
	SophCo, Inc.
	Sota Miltope
	Stellar Systems Inc.
	Sterling Software Inc. (Dylakor Division)
	Sterling Software Inc. (System SW Marketing Division)
	SunSoft
	Symantec
	TRW, Electronic Product Ltd.
	Techmar Computer Products, Inc.
	Techmatics, Inc.
	Technical Communications Corp.
	Telequip Corp.
	Thumbscan, Inc.
	Trigram Systems
	Trintron Sytems
	Trusted Information Systems, Inc.

USA	UTI-MACO Safeguard Systems
	UUNet Technologies, Inc.
	United Software Security
	VLSI
	Verdix Corp.
	Visionary Electronics
	Wang Laboratories
	Western DataCom Co. Inc.
	WordPerfect
	XTree
	Yeargin Engineering
	hDC
	usrESZ Software, Inc.
YUGOSLAVIA	Sophos Yu d.o.o.

ATTACHMENT 3

Excerpts from Recent National Research Council Studies Regarding Export Control and Cryptography

- Computers at Risk: Safe Computing In the Information Age, published by the National Academy Press, Washington, D.C., 1991.

  From "Recommendations":

  Recommendation 4 (p. 37): **Clarify Export Control Criteria, and Set Up a Forum for Arbitration.**

  Subsection 4b (p. 38): **Review export controls on implementations of the Data Encryption Standard.** The growth of networked and distributed systems has created needs for encryption in the private sector. Some of that pressure has been seen in the push for greater exportability of products using the Data Encryption Standard (DES) and its deployment in foreign offices of U.S. companies.

  In principle, any widely available internationally usable encryption algorithm should be adequate. NIST, working with NSA, is currently trying to develop such algorithms. However, the committee notes that this effort may not solve industry's problems, for several reasons. The growing installed base of DES products cannot be easily retrofitted with the new products. The foreign supply of DES products may increase the appeal of foreign products. Finally, NSA influenced alternatives may be unacceptable to foreign or even U.S. buyers, as evidenced by the American Banking Association's opposition to the NSA's proposals to effectively restrict banks to encryption algorithms designed and developed by NSA when the DES was last recertified, in 1988.

  The committee has been apprised that NSA, because of classified national security concerns, does not support the removal of remaining restrictions on export of DES. However, there is a growing lack of sympathy in the commercial community with the NSA position on this matter. The committee recommends that the Administration appoint an arbitration group consisting of appropriately cleared individuals from industry and the Department of Commerce as well as the Department of Defense to impartially evaluate if there are indeed valid reasons at this time for limiting the export of DES.

- Global Trend in Computer Technology and Their Impact on Export Control, published by the National Academy Press, Washington, D.C., 1988.

  From "Data Encryption Standard" (p. 122):

  The International Traffic in Arms Regulations (ITAR) require export license for U.S. products using DES, and this appears to be a case of unnecessary export control diminishing U.S. competitiveness. DES or comparable cryptography is available from multiple international vendors.

- Finding Common Ground: U.S. Export Controls in a Changed Global Environment, published by the National Academy Press, Washington, D.C., 1991.

  From Appendix C, "Computer Networks" (p. 260):

  If foreign encryption technology is imported into the United States to meet ISO standards but is prohibited from use by ITAR regulations, U.S. industry, the U.S. government, and other users will be isolated from the worldwide network for much of the future commerce that increasingly will use such technology. Further, U.S. industry will be unable to manufacture and export compatible equipment to compete in the world market.

  *** Existing ITAR regulations should be revised to enable the use of high-quality encryption protocols for the worldwide network. Otherwise, U.S. interests will be sidestepped by ISO encryption schemes and standards currently progressing internationally.**

- Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition, published by the National Academy Press, Washington, D.C., 1987.

  From "Recommendations":

  Subsection 4 (p. 170): **Remove Items Whose Control Is No Longer Feasible.** ...the United States should actively seek to remove from both the U.S. Control List and the CoCom International List items whose control is no longer feasible or necessary. This would include goods and technologies:

  - for which there is demonstrated foreign availability from any country that has not agreed to adhere to export controls and for which this availability has not been eliminated within a reasonable period of time through negotiated agreements....

From subsection II (p. 173): ACCORD GREATER IMPORTANCE IN U.S. NATIONAL SECURITY EXPORT CONTROL DECISIONS TO MAINTAINING U.S. TECHNOLOGY STRENGTH, ECONOMIC VITALITY AND ALLIED UNITY.

The panel recommends that executive branch decisions concerning national security export controls accord greater importance than they currently do to maintaining U.S. technological strength, economic vigor, and allied unity.

* * *

* * * * * * *

Toward these ends, the panel recommends the following specific changes in U.S. policy and procedures.

1. **Balance the Protection of Military Security with the Promotion of National Economic Vitality Through Affirmative Policy Direction....**

ATTACHMENT 4

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION #1

March 18, 1992

The Board has examined the present status of the proposed Digital Signature Standard (DSS) being undertaken b the National Institute of Standards and Technology (NIST). In view of:

(1) the significant public policy issues raised during the review of the proposed standard;

(2) the increasingly pervasive use of digital technologies;

(3) the potential impacts upon the security of the unclassified/sensitive government community;

(4) the relationship of the DSS to the existing NIST cryptographic security program; and

(5) the posture of the U.S. in international commerce.

THE BOARD FINDS THAT:

(1) a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required. This national level review must involve the national security, law enforcement, government unclassified/sensitive, and commercial communities. Representative from the private sector should include both vendors and users. In the next several months, NIST/NSA should sponsor a workshop on the widespread use of cryptography. This national review should be concluded by June 1993 and should result in a national policy concerning the use of cryptography in unclassified/sensitive government and the private sector.

(2) NIST has made significant progress in resolving the technical issues related to the proposed DSS. The Board recommends that NIST continue to seek resolution of the patent, infrastructure, and other remaining issues raised during the public comment process. The Board recognizes that much of the work, and in particular the infrastructure, is algorithmic independent and must be continued by NIST to assure timely implementation of digital signature technology within the government.

FOR: Colvin, Gallagher, Gangemi, Kuyers, Lipner, Philcox, Rand, Walker, Willis, and Zeitler
AGAINST: None ABSTAIN: None

Motion Unanimously Approved.

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION 93-5

September 1-2, 1993

Subsequent to the June 2-4, 1993 meeting of the CSSPAB, the Board has held an additional 4 days of public hearings and has collected additional public input.

The clear message is that the preliminary concerns stated in Resolution 1 of that date have been confirmed as serious concerns which need to be resolved.

Public input has heightened the concerns of the Board to the following issues:

- A convincing statement of the problem that Clipper attempts to solve has not been provided.
- Export and import controls over cryptographic products must be reviewed. Based upon data compiled from U.S. and international vendors, current controls are negatively impacting U.S. competitiveness in the world market and are not inhibiting the foreign production and use of cryptography (DES and RSA).
- The Clipper/Capstone proposal does not address the needs of the software industry, which is a critical and significant component of the National Information Infrastructure and the U.S. economy.
- Additional DES encryption alternatives and key management alternatives should be considered since there is a significant installed base.
- The individuals reviewing the Skipjack algorithm and key management system must be given an appropriate time period and environment in which to perform a thorough review. This review must address the escrow protocol and chip implementation as well as the algorithm itself.
- Sufficient information must be provided on the proposed key escrow scheme to allow it to be fully understood by the general public.
- Further development and consideration of alternatives to the key escrow scheme need to be considered, e.g., three "escrow" entities, one of which is a non-government agency, and a software based solution.
- The economic implications for the Clipper/Capstone proposal have not been examined. These costs go beyond the vendor cost of the chip and include such factors as customer installation, maintenance, administration, chip replacement, integration and interfacing, government escrow system costs, etc.
- Legal issues raised by the proposal must be reviewed.

Congress, as well as the Administration, should play a role in the conduct and approval of the results of the review.

Moreover, the following are additional concerns of the Board:

- Implementation of the Clipper initiative may negatively impact the availability of cost-effective security products to the U.S. Government and the private sector;

and

- Clipper products may not be marketable or usable worldwide.

FOR:	Castro, Gangemi, Lambert, Lipner, Kuyers, Philcox, Rand, Walker, Whitehurst, and Zeitler
AGAINST:	none
ABSTAIN:	Gallagher
ABSENT:	Colvin

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION 93-6

SEPTEMBER 1-2, 1993

The Board believes that in deciding cryptographic policies and standards in the U.S., there is a compelling need to consider and evaluate the concerns listed below. We, therefore, endorse the process being pursued by the administration in the form of an interagency review but believe the scope of that review needs to include adequate industry input. We reaffirm our recommendation (of March 1992) that the issues surrounding this policy be debated in a public forum. In view of the worldwide significance of these issues the Board believes that the Congress of the U.S. must be involved in the establishment of cryptographic policy.

The Board, furthermore, believes that there are a number of issues that must be resolved before any new or additional cryptographic solution is approved as a U.S. government standard:

1. The protection of law enforcement and national security interests;
2. The protection of U.S. computer and telecommunication interests in the international marketplace; and
3. The protection of U.S. persons' interests both domestically and internationally.

FOR: Castro, Gallagher, Gangemi, Lambert, Lipner, Kuyers, Philcox, Rand, Walker, Whitehurst, and Zeitler

AGAINST: none

ABSTAIN: none

ABSENT: Colvin

Testimony of Philip Zimmermann to Subcommittee for Economic Policy, Trade, and the Environment
US House of Representatives
12 Oct 1993

Mr. Chairman and members of the committee, my name is Philip Zimmermann, and I am a software engineer who specializes in cryptography and data security. I'm here to talk to you today about the need to change US export control policy for cryptographic software. I want to thank you for the opportunity to be here and commend you for your attention to this important issue.

I am the author of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world and has since become the de facto worldwide standard for encryption of E-mail. The US Customs Service is investigating how PGP spread outside the US. Because I am a target of this ongoing criminal investigation, my lawyer has advised me not to answer any questions related to the investigation.

I. The information age is here.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers, because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country. Governments formed their attitudes toward cryptographic technology during this period. And these attitudes persist today. Why would ordinary people need to have access to good cryptography?

Another problem with cryptography in those days was that cryptographic keys had to be distributed over secure channels so that both parties could send encrypted traffic over insecure channels. Governments solved that problem by dispatching key couriers with satchels handcuffed to their wrists. Governments could afford to send guys like these to their embassies overseas. But the great masses of ordinary people would never have access to practical cryptography if keys had to be distributed this way. No matter how cheap and powerful personal computers might someday become, you just can't send the keys electronically without the risk of interception. This widened the feasibility gap between Government and personal access to cryptography.

Today, we live in a new world that has had two major breakthroughs that have an impact on this state of affairs. The first is the coming of the personal computer and the information age. The second breakthrough is public-key cryptography.

With the first breakthrough comes cheap ubiquitous personal computers, modems, FAX machines, the Internet, E-mail, digital cellular phones, personal digital assistants (PDAs), wireless digital networks, ISDN, cable TV, and the data superhighway. This information revolution is catalyzing the emergence of a global economy.

But this renaissance in electronic digital communication brings with it a disturbing erosion of our privacy. In the past, if the Government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This is analogous to catching fish with a hook and a line, one fish at a time. Fortunately for freedom and democracy, this kind of labor-intensive monitoring is not practical on a large scale.

Today, electronic mail is gradually replacing conventional paper mail, and is soon to be the norm for everyone, not the novelty it is today. Unlike paper mail, E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. This is analogous to driftnet fishing — making a quantitative and qualitative Orwellian difference to the health of democracy.

The second breakthrough came in the late 1970s, with the mathematics of public key cryptography. This allows people to communicate securely and conveniently with people they've never met, with no prior exchange of keys over secure channels. No more special key couriers with black bags. This, coupled with the trappings of the information age, means the great masses of people can at last use cryptography. This new technology also provides digital signatures to authenticate transactions and messages, and allows for digital money, with all the implications that has for an electronic digital economy. (See appendix)

This convergence of technology — cheap ubiquitous PCs, modems, FAX, digital phones, information superhighways, et cetera — is all part of the information revolution. Encryption is just simple arithmetic to all this digital hardware. All these devices will be using encryption. The rest of the world uses it, and they laugh at the US because we are railing against nature, trying to stop it. Trying to stop this is like trying to legislate the tides and the weather. It's like the buggy whip manufacturers trying to stop the cars — even with the NSA on their side, it's still impossible. The information revolution is good for democracy — good for a free market and trade. It contributed to the fall of the Soviet empire. They couldn't stop it either.

Soon, every off-the-shelf multimedia PC will become a secure voice telephone, through the use of freely available software. What does this mean for the Government's Clipper chip and key escrow systems?

Like every new technology, this comes at some cost. Cars pollute the air. Cryptography can help criminals hide their activities. People in the law enforcement and intelligence communities are going to look at this only in their own terms. But even with these costs, we still can't stop this from happening in a free market global economy. Most people I talk to outside of Government feel that the net result of providing privacy will be positive.

President Clinton is fond of saying that we should "make change our friend." These sweeping technological changes have big implications, but are unstoppable. Are we going to make change our friend? Or are we going to criminalize cryptography? Are we going to incarcerate our honest, well-intentioned software engineers?

Law enforcement and intelligence interests in the Government have attempted many times to suppress the availability of strong domestic encryption technology. The most recent examples are Senate Bill 266 which mandated back doors in crypto systems, the FBI Digital Telephony bill, and the Clipper chip key escrow initiative. All of these have met with strong opposition from industry and civil liberties groups. It is impossible to obtain real privacy in the information age without good cryptography.

The Clinton Administration has made it a major policy priority to help build the National Information Infrastructure (NII). Yet, some elements of the Government seems intent on deploying and entrenching a communications infrastructure that would deny the citizenry the ability to protect its privacy. This is unsettling because in a democracy, it is possible for bad people to occasionally get elected — sometimes very bad people. Normally, a well-functioning democracy has ways to remove these people from power. But the wrong technology infrastructure could allow such a future government to watch every move anyone makes to oppose it. It could very well be the last government we ever elect.

When making public policy decisions about new technologies for the Government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the Government to deploy those technologies. This is simply a matter of good civic hygiene.

II. Export controls are outdated and are a threat to privacy and economic competitiveness.

The current export control regime makes no sense anymore, given advances in technology.

There has been considerable debate about allowing the export of implementations of the full 56-bit Data Encryption Standard (DES). At a recent academic cryptography conference, Michael Wiener of Bell Northern Research in Ottawa presented a paper on how to crack the DES with a special machine. He has fully designed and tested a chip that guesses DES keys at high speed until it finds the right one. Although he has refrained from building the real chips so far, he can get these chips manufactured for $10.50 each, and can build 57000 of them into a special machine for $1 million that can try every DES key in 7 hours, averaging a solution in 3.5 hours. $1 million can be hidden in the budget of many companies. For $10 million, it takes 21 minutes to crack, and for $100 million, just two minutes. That's full 56-bit DES, cracked in just two minutes. I'm sure the NSA can do it in seconds, with their budget. This means that DES is now effectively dead for purposes of serious data security applications. If Congress acts now to enable the export of full DES products, it will be a day late and a dollar short.

If a Boeing executive who carries his notebook computer to the Paris air show wants to use PGP to send email to his home office in Seattle, are we helping American competitiveness by arguing that he has even potentially committed a federal crime?

Knowledge of cryptography is becoming so widespread, that export controls are no longer effective at controlling the spread of this technology. People everywhere can and do write good cryptographic software, and we import it here but cannot export it, to the detriment of our indigenous software industry.

I wrote PGP from information in the open literature, putting it into a convenient package that everyone can use in a desktop or palmtop computer. Then I gave it away for free, for the good of our democracy. This could have popped up anywhere, and spread. Other people could have and would have done it. And are doing it. Again and again. All over the planet. This technology belongs to everybody.

III. People very badly want their privacy.

PGP has spread like a prairie fire, fanned by countless people who fervently want their privacy restored in the information age.

Today, human rights organizations are using PGP to protect their people overseas. Amnesty International uses it. The human rights group in the American Association for the Advancement of Science uses it.

Some Americans don't understand why I should be this concerned about the power of Government. But talking to people in Eastern Europe, you don't have to explain it to them. They already get it — and they don't understand why we don't.

I want to read you a quote from some E-mail I got last week from someone in Latvia, on the day that Boris Yeltsin was going to war with his Parliament:

> "Phil I wish you to know: let it never be, but if dictatorship takes over Russia your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks."

Appendix — How Public-Key Cryptography Works

In conventional cryptosystems, such as the US Federal Data Encryption Standard (DES), a single key is used for both encryption and decryption. This means that a key must be initially transmitted via secure channels so that both parties have it before encrypted messages can be sent over insecure channels. This may be inconvenient. If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?

In public key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key. Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the same kind of secure channels that a conventional cryptosystem requires.

Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. No one but the recipient can decrypt it, because no one else has access to that secret key. Not even the person who encrypted the message can decrypt it.

Message authentication is also provided. The sender's own secret key can be used to encrypt a message, thereby "signing" it. This creates a digital signature of a message, which the recipient (or anyone else) can check by using the sender's public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. Forgery of a signed message is infeasible, and the sender cannot later disavow his signature.

These two processes can be combined to provide both privacy and authentication by first signing a message with your own secret key, then encrypting the signed message with the recipient's public key. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. These steps are done automatically by the recipient's software.

STATEMENT OF

DON HARBERT
VICE PRESIDENT, SOFTWARE ENGINEERING
DIGITAL EQUIPMENT CORPORATION

ON

ENCRYPTION EXPORT CONTROLS

BEFORE THE
SUBCOMMITTEE ON ECONOMIC POLICY, TRADE,
AND THE ENVIRONMENT

HOUSE COMMITTEE ON FOREIGN AFFAIRS

OCTOBER 12, 1993

I am Don Harbert, Vice President, Software Engineering, Digital Equipment Corporation. Thank you for the opportunity to present our views on the important subject of export controls on encryption products. Digital Equipment is the leading worldwide supplier of networked computer systems, software and services, and leads the industry in interactive, distributed and multivendor computing. Digital is an international company and now derives roughly 63% of its revenue from outside of the U.S. Digital produces both encryption hardware and software, and is itself a user of data security products based on encryption techniques.

U.S. export controls on encryption products must be brought into line with reality. Many existing controls are ineffective, and no longer enhance national security objectives in any meaningful way. These controls do, however, encourage the development of encryption products outside the U.S., and needlessly deprive U.S. companies of significant export opportunities in some of America's largest overseas markets. It is time for a serious reexamination of controls on encryption.

The market for encryption products both outside and inside the U.S. is significant. While the need for secure communications by government entities is well recognized, this capability is just as important to an ever-widening range of organizations in the private sector. In general, any group that employs data communications and is dependent on valuable proprietary knowledge is vulnerable to unauthorized access to that data.

Commercial activities that fall into this category are legion. The banking industry, for example, is a major market for encryption. In addition, non-banking industries with a history of industrial espionage such as the automobile, petrochemical and pharmaceutical industries are also established markets. Guides, manuals and other instructional materials dealing with encryption, as well as software packages themselves containing encryption functions, are common fare in retail software outlets in the U.S., Europe and elsewhere around the world.

While a limited number of encryption applications are under the jurisdiction of the Department of Commerce, most file (or data) encryption is subject to control under the Arms Export Control Act, administered by the Department of State. Software containing file encryption, including software that is in the public domain or that is "mass-market" (by the internationally accepted COCOM definition) is subject to the same severe licensing regime as are tanks and missiles.

The export licensing regime for munitions administered by the Department of State is even slower, more restrictive and more cumbersome than that for commercial products administered by the Department of Commerce. An even more important problem, however, is the policy of license denial for non-bank commercial customers.

The National Security Agency reviews export licenses and sets policy for the export of encryption products. NSA routinely recommends denial of exports to commercial customers, even those located in America's closest allied countries. And, with the exception of a small number of weak encryption products, NSA will approve exports of file encryption products to only nine allied governments, banks, and subsidiaries of U.S. companies. Thus, not only are these products subject to harsher controls, but there is a de facto embargo of them to America's major commercial data processing markets in Western Europe and Japan.

In part as a result of NSA's embargo policy, a data security industry has developed overseas, free from competition from U.S. companies (particularly in their home markets) and completely free from U.S. export controls. Large multinational corporations as well as smaller specialized firms provide security products in response to growing demand, and make them available domestically without hindrance. A recent study by the Software Publishers Association cited 193 companies outside of the U.S. that produce cryptographic products, including a large number offering products based on the U.S. Data Encryption Standard.

Export controls do exist on encryption products among all of America's major allies; however, the nature and severity of controls varies significantly. Britain and Japan, for example, control encryption as a dual use, not a munitions, item. Other countries, like France, Germany and Holland, have export controls on shipment of encryption products similar to those of the U.S.

However, it is very important to note that with the exception of France, none of these U.S. allies impose restrictions on the use of encryption within its own borders. As a result, data security markets within these countries are guaranteed to local producers because of the NSA-imposed embargo of products of U.S. producers.

Encryption controls impact the computer industry in a number of important ways. The following cases demonstrate the major impacts that aspects of current controls have on the industry.

Case 1: Leveraged Sales

For many large computer companies like Digital, direct revenue from from the sale of data security products is limited; the market is in fact dominated by specialty firms. Large sales are, however, often dependent on our ability to offer encryption as a feature of a customer "solution" incorporating hardware, software and services. Thus, if we are unable to offer an encryption solution, significant loss of revenue may result, even though the encryption/hardware and software element of the deal may be minor.

Typical examples include replacement of corporate data systems, infrastructure projects such as PTT (post, telephone and telegraph) installations, and cellular telephone network operations. For such projects, where overseas customers perceive data security as necessary, they will be forced to look to a non-U.S. vendor for the entire project.

Digital has been directly and negatively affected by an inability to offer file encryption as an element of large integration projects overseas. Over the last twelve months, we have lost up to $70 million in contracts from West European customers because of our inability to deliver encryption as part of a total solution. In addition, we have not pursued a number of inquiries from government and civilian customers for similar projects because of the certain knowledge that an export license for the required encryption component of the project would not be approved for export.

Case 2: Public Domain Software

The U.S. Munitions List controls software containing file encryption even if it is in the public domain (i.e., generally available to the public through libraries, universities, and other public releases). As a result, a number of products are available and widely distributed on international networks such as the INTERNET that contain ITAR-controlled encryption functionality. Companies like Digital, which access public domain software for internal research purposes, must screen thousands of public domain software applications for encryption in order to keep it out of their international networks and so avoid unintentional export compliance incidents.

Case 3: Mass-market Software

Software that is not in the public domain, but that is generally available to the public through retail channels and needs no significant support by the vendor ("mass-market" software) is beyond effective control. These packages are low-cost, marketed in the thousands or tens of thousands, and move readily across national borders over international computer networks and in personal baggage.

COCOM recognized both the practical limitations of controlling such software and the seriously adverse effects of maintaining controls. As a result, COCOM (with the U.S.) adopted the "General Software Note," which frees such software from validated licensing requirements. However, for U.S. export control purposes, this note does not apply to mass-market software containing encryption capability, even though the rationale for decontrol is just as as valid.

A Need for Change

Digital recognizes the need to retain some controls on encryption products in the interests of national security. A number of useful changes in current policy can, however, be made to rationalize the current system. The changes I will outline would allow U.S. companies to compete for business abroad where data security is a factor, but will retain controls on that which is controllable.

1. **The U.S. should shift jurisdiction for controls of dual-use encryption to the Department of Commerce**

Encryption has established commercial applications, is widely used in commercial contexts, and is specifically controlled by COCOM as a commercial, not a munitions item. Commerce control would not preclude NSA participation in the licensing process, but would mean more flexibility in license authorizations, and more likelihood that commercial and economic needs were at least considered in individual export licensing decisions.

2. **Expand categories of overseas customers for whom export licenses my be approved.**

Export licenses for encryption products, including those based on the Data Encryption Standard, may now be approved to banks in a range of countries. This policy of approval should be extended to other customers, including large multinational firms and governments outside the approved nine for some applications. Subject to government review, reliable customers in countries like Britain, Germany and Japan should be allowed access to data security products produced in the U.S., and should not be forced to turn to non-U.S. suppliers as a result of the NSA embargo.

3. Decontrol encryption software in the public domain

Encryption software that is in the public domain, or which is generally available to the interested public without restriction, is beyond effective control regardless of its technical characteristics. Dual-use public domain software is not controlled by the U.S. in any other context other than encryption, and is not controlled by COCOM. To continue controls on such products serves no national security purpose and invites needless compliance risk for those using otherwise uncontrolled international networks.

4. Relax controls on mass-market software containing encryption

The U.S. and its COCOM allies have recognized that "mass-market" products are also beyond effective control, and for that reason have afforded such software much less stringent licensing treatment. Consistent with controls on other commercial software, we recommend that validated licensing requirements for software containing encryption that qualifies as "mass-market" by the accepted U.S. and COCOM definition be removed for all but states supporting international terrorism and embargoed countries.

In conclusion, U.S. export controls on encryption must be changed to reflect technological and market reality. Controls that are no longer effective do not contribute to the national security. They do contribute to the proliferation of data security vendors outside the U.S., and they do impede the ability of America's leading computer companies to compete in their largest international markets. It is time for a change.

FROST & SULLIVAN, Inc.

The Demand for Information Security and Encryption in Fortune 500 Companies in the United States

Prepared for

the Business Software Alliance

October 1, 1993

Demand for Information Security and Encryption in Fortune 500 Companies in the United States

Research Design

Frost & Sullivan was commissioned by The Business Software Alliance (hereafter referred to as BSA) to conduct research and provide realistic and unbiased information on the market demand for data security and encryption in Fortune 500 companies in the United States.

Working in concert, BSA and Frost & Sullivan designed a list of questions to determine information including:

- The importance of information security to companies
- The importance of encryption as a software capability
- The willingness of customers to purchase foreign programs otherwise perceived as less desirable if they include strong security

Approximately 200 companies were contacted in order to discuss their current and future needs for data security and encryption software. The people contacted were typically either MIS managers or other key representatives within the MIS department of the companies contacted.Out of the 201 contacts interviewed, only 151 felt comfortable enough with discussing their company's data security information. The contacts that were unable to respond were more than willing to discuss this issue, but could not answer any specific questions due to the sensitive nature of the subject.

The companies that were interviewed covered a broad spectrum of industries, specifically including:

- Manufacturing
- Healthcare and allied businesses
- Financial and allied businesses

The companies interviewed were about evenly divided between those with and without extensive overseas operations.

Results Summary

More than 90 percent of the interviewees said that information security was important to their operations, and 78 percent said this covered elctronic communication with vendors and customers as well. Almost one-half specifically stated that data encryption was important to protect the security of their information in addition to password or access control. Indeed, over one-third said they look for encryption capabilities when buying software and that they would consider purchasing foreign software with otherwise less desirable features if that software offered data security not available in a U.S. program! Combined with the ever increasing need to communicate electronically, increasing demand for software with encryption capabilities seems assured.

Importance of Data Security

Of the 151 completed interviews, 139 respondents (92.1 percent) feel that information security is important to their company's operations, and 117 respondents (77.5 percent) felt that information security was very important. Only 6 percent felt that it was marginally important, and 5.3 percent of respondents stated that information security was not important to their company's operations.

Importance of Electronic Communication

The importance of communicating electronically corporate-wide, as well as communicating with outside entities such as vendors and customers, was also given a high degree of importance. 90 percent of the contacts interviewed felt that it was important to communicate electronically corporate-wide, and 78.2 percent stated that it was important to communicate with outside entities (customers, suppliers) as well.

Need for Software Encryption Capabilities

To best determine the importance and extent of software data encryption requirements and desires, Frost & Sullivan asked several similar questions. First, we asked the contact if data encryption was important to protect the security and confidentiality of information in addition to password or access control. We then asked whether one feature they look for when buying software is the ability to encrypt information when purchasing software.

We found that 70 contacts (46.4 percent) believed that data encryption was important to protect the security and confidentiality of information in addition to passwords and access control. 37.1 percent of the contacts stated that they looked for the ability to encrypt information in software, with another 7.9 percent saying that the answer was proprietary and did not respond to this particular question.

Adverse Impact on the U.S. Software Industry

We then asked the interviewees if they would consider purchasing software manufactured offshore that had less desirable features if domestic programs lacked sufficient security capabilities, due to controls placed on domestic manufacturers by the U.S. government.

Several interviewees displayed discomfort when asked if they would consider purchasing foreign software with data security capability but otherwise less desirable features. Indeed, 31 contacts refused to answer this particular question. However, 56 said that they would consider purchasing foreign software in these circumstances. 64 contacts stated that they would not consider purchasing in such a situation.

Implications of Encryption Policy on the National Information Infrastructure

Martin E. Hellman[1]

Electronic information processing is replacing paper in a number of applications. Ten years ago, fax was used primarily by large law offices and a few other professionals; today, most businesses could not compete without it. Electronic mail is rapidly moving from a curiosity of the academic community to a mainstream business application. Widespread electronic document distribution, including multimedia messages, is on the near horizon. Figure 1 on the next page illustrates the rapid growth of information flowing over the Internet computer-communications network and shows that, today, it carries approximately thirty-five *billion* packets per month.

Electronic communication has a number of advantages which are fueling this rapid switch from paper-based communications.

- **Speed:** electronic messages move at the speed of light. Paper moves at the speed of the Postal Service, or if premium prices are acceptable, overnight.
- **Cost:** Faxing a single page across the country costs as much as a first class stamp. E-mail can send on the order of 100 pages for the same amount.
- **Storage:** An 8 mm tape cartridge that sells for $10 and is the size of an

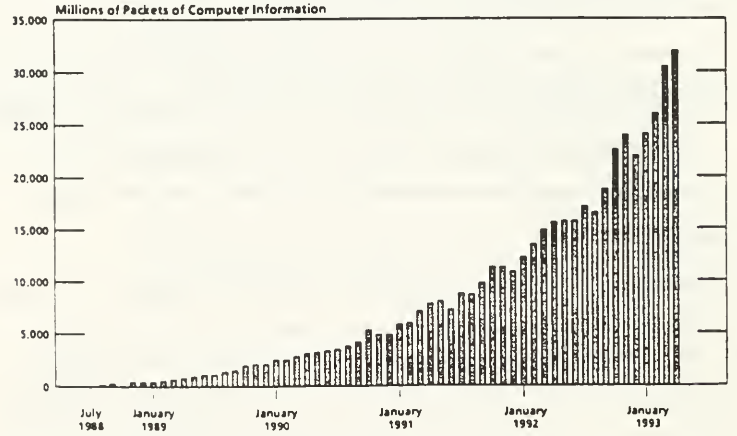
---

[1] Martin E. Hellman, Professor of Electrical Engineering at Stanford University, has worked in cryptography for over twenty years. His contributions, notably his invention with Whit Diffie and Ralph Merkle of "public key" cryptography has received a number of honors from the IEEE (Institute of Electrical and Electronics Engineers, the primary Electrical Engineering professional society): He was elected a Fellow of the IEEE "for contributions to cryptography;" received two IEEE awards for outstanding papers, and was awarded an IEEE Centennial Medal. The California State Psychological Association also honored him with its first Award for Distinguished Contributions to Consumer Protection. Before joining Stanford's faculty in 1971, Prof. Hellman was on the faculty at MIT (1969-71) and the research staff at IBM (1968-69). Preparation of this report was supported by the Business Software Alliance.

audio cassette can store 10 Gbytes of data, equivalent to 10,000,000 pages of text, or a thousand file drawers, each stuffed to the gills.

- **Access:** Electronic files can be accessed more rapidly and more conveniently than paper. When a copy is brought "on-screen," the original resides safely on disk, whereas a paper copy that is accessed is vulnerable to loss or misfiling when returned to storage.
- **Content-Based Access :** Access based on content (e.g., "Find all documents containing the words *National Information Infrastructure*.") is not economically feasible with paper documents, but can be accomplished inexpensively with computer-readable information.
- **Reproducibility:** Each copy of a paper document is degraded somewhat, while a tenth-generation copy of a digital document is indistinguishable from the original.

Summary Figure 1.
History of Internet Traffic, 1988-1993



SOURCE Congressional Budget Office from data provided by Merit/NSFNET, Ann Arbor, Michigan

Figure 1. History of Internet Traffic, 1988-1993. [Source: Congressional Budget Office from data provided by Merit/NSFNET, Ann Arbor, MI.]

Recognizing these advantages and their importance in maintaining America's competitiveness, the Clinton Administration has proposed the development of a National Information Infrastructure (NII), sometimes referred to as an electronic counterpart to the Interstate Highway System. This initiative is to be commended. But, unless the Clinton Administration reverses existing national policy which discourages the use of encryption (scrambling to protect information), it will get an insecure NII and three possible embarrassments:

- **A White Elephant:** Just as people do not use post cards for most of their mail, prudent users will refuse to trust most information to an insecure NII.
- **A Disaster:** Careless or ignorant users who trust confidential or valuable information to an insecure NII will be easy prey to hackers, thieves, spies, or others who violate the system.
- **Foreign Dominance:** Foreign companies, operating from countries which do not discourage encryption, could offer a competing, secure service and put the NII out of business.

An insecure NII is extremely dangerous because the advantages of electronic communication listed above are even more valuable to illegitimate users ("spies") than to authorized users. Once an electronic message has been intercepted, a spy can send an exact replica of the original, rapidly and inexpensively, to his headquarters. There it can be stored inexpensively and accessed conveniently. Fast, inexpensive access based on message content is indispensable to spies because they must sort through millions of irrelevant messages to find one of interest (e.g., any message containing the words *Clinton, reelection, California,* and *strategy*). Approximately ten billion words of computer-readable messages, such as e-mail, can be scanned for a dollar, so even if only one message in a million is of interest, $1 worth of scanning produces

10,000 interesting words![2]

Even though scanning is surprisingly cheap, we still would be safe if it were expensive or difficult for a spy to intercept our message stream. Unfortunately, interception is also extremely cost-effective in many instances. The increasing use of wireless and other shared communication channels (e.g., Local Area Networks or LAN's) increases the vulnerability of electronic communications by making large amounts of information available to unintended users without wiretaps or other risky operations.

Communications carried by satellite can be picked up by inexpensive "dishes" hundreds of miles from the intended recipient and give the spy access to literally billions of words per day. Cellular telephone conversations are vulnerable, as Princess Di and Governor Wilder now realize. Local area networks are, in reality, spy networks in which each node watches all the information flowing over the shared cable and picks out only those messages with its address. It would take only minor modifications to create phantom nodes that watch all information flowing over the cable and pick out only those intended for someone else on the network (e.g., I could intercept all messages intended for the president of Stanford University). Because such phantom nodes look like normal nodes, it would be hard to detect their existence. The same is true for interception of satellite and cellular telephone messages. Spying is a passive activity, and therefore hard to detect.

More ominously the Internet, on which the NII is likely to be modeled, uses distributed communication and switching. In this approach, the computer at Stanford which holds my e-mail is also used as a switch, for example taking messages from the University of Washington, 800 miles north of us, and relaying them to UCLA, 400 miles to the south. This provides fault tolerance (if Stanford's node goes down, any other "gateway" south of the University of Washington can be used as the relay) and cost savings (e-mail from the University of Washington to UCLA can make use of unused capacity in Stanford's communication lines and does not need a separate, dedicated link). But, while the University of Washington's messages are being relayed by these other machines, they are vulnerable to search for key words that sort out "interesting" messages. Any Stanford "super-user" – and there are a number of them – can listen in on all the traffic passing through Stanford.

---

[2] In a timed experiment, my NeXT workstation searched approximately a million characters per second. This is equivalent to 100 billion characters per day, or 200 trillion characters over its approximately five year expected life. At six characters per average word, this $3,000 machine can search 30 trillion words over its life, resulting in the 10 billion words per dollar quoted above. Because these are only approximate numbers intended to give ball park figures, only one decimal place of accuracy has been maintained (i.e., they are accurate to "one significant figure").

If the NII is developed under current policy, using it will be worse than writing all paper-based communications on post cards because a spy need not be physically present in the "Post Office" to intercept your "post cards." The NII will therefore be a tempting target for foreign intelligence organizations, organized crime (for blackmail, insider information, and sale of strategic business information), competing companies, and so-called "hackers." NSA (the National Security Agency) is well aware of the dangers inherent in electronic mail and prohibits its own confidential information from being sent over the Internet. Instead, the Agency uses its own secure e-mail network and is extremely careful to prevent any connection between the two.

While NSA has generally resisted the spread of commercial and private encryption, it has made an exception with respect to the communications of DoD contractors and other private-sector communications deemed of national security concern. NSA has warned a number of such concerns to encrypt or otherwise protect their communications that were being spied upon by NSA's foreign counterparts. While the Soviet Union and its satellites used to be NSA's prime concern, the French government is a major threat today, gleaning economic and technological intelligence from American companies and passing this information on to their French competitors.

If all messages flowing through the NII are encrypted then the insecurity currently present in the Internet would disappear. The Administration recently released a report entitled *The National Information Infrastructure: Agenda For Action* which acknowledges this need: "The trustworthiness and security of communications channels and networks are essential to the success of the NII." But when the report calls for "review of encryption technology," it merely says that "In April, the President announced a thorough review of Federal policies on encryption technology." While there may be other April Administration actions that are referred to, the only one of which I am aware (the "Clipper chip" announcement) *discouraged* private-sector encryption by adding a new encryption system (the Clipper chip) which is incompatible with existing systems based on the Data Encryption Standard or DES. This action will likely retard the growth of encryption as companies and individuals delay purchase, waiting to see which of these mutually incompatible systems will dominate. The Clipper system also has a major drawback when applied to securing the Internet or NII: Clipper is a secret algorithm, available only in silicon, and cannot be implemented in software. Yet software encryption is most easily, cheaply, and rapidly implemented on such networks, requiring only an update to software releases. If encryption hardware must be installed at every node, security is likely to be delayed for years, and may never become widespread.

If the Administration decides to reverse current government policy which discourages encryption, then the required technology is in hand. While popular accounts of encryption often give the impression first popularized by Edgar Allen Poe that "human ingenuity cannot concoct a cipher which human ingenuity cannot resolve," Poe was wrong. Encryption is a special form of computation and has benefitted every bit as much as word processing from the rapid decrease in the cost of computation. Ciphers that cannot be broken with any foreseeable technology can be implemented inexpensively today. When implemented in software, encryption is an almost-free add-on to a backup utility, telecommunications package, or similar program.

The former high cost of key distribution, in which couriers had to communicate the secret keys used to encrypt and decrypt message (analogous to "combinations" used to "lock" and "unlock" messages), can be eliminated by public key systems. In a public key system, two users communicating across an insecure channel *without any prearrangement* are able to agree on a secret key that an eavesdropper is unable to determine. This seemingly impossible feat is accomplished by allowing the eavesdropper to recover the key in theory, but preventing him from doing so in practice by making the cost of recovery prohibitive – for example, more than the entire country's GNP.[3]

Public key systems also allow digital signatures, numbers appended to digital messages which can easily be checked by anyone as authenticating that the message originated from its claimed source, but which can be easily generated only by the legitimate signer. Digital signatures are tied to message content, so that the recipient of an electronic bank draft cannot change the amount or any other part of the check.

Digital signatures are generated with a user-specific, secret key. They are validated with a related, public key. While, in theory, the secret signing key can be derived from the public validating key, again that can be prevented in practice by making the derivation ridiculously expensive. Digital signatures promise to revolutionize business by allowing electronic contracts, tax returns, etc. In some ways, digital signatures are more secure than written signatures: Because written signatures are not message dependent, one signed paper document allows unlimited imitations by a skilled forger. Digital signatures do not suffer from this problem.

---

[3] For example, the RSA public key system depends on the difficulty of factoring large integers. If I ask you to multiply 13 times 29, it takes only a short time to find the product: 13 x 29 = 377. But it takes much longer if I give you 377 and ask you to find its two factors, 13 and 29. Similarly, a computer can multiply two 100-digit numbers in a matter of milliseconds, but would take over a million years to factor the 200-digit product.

At this point it might be asked why, if cryptography is so needed, it is not more evident in our lives. The answer is two-fold. First, cryptography is more widespread than we realize since it is often done automatically, in which case it is invisible to the user. Anyone who has used Lotus' *Notes*™ has used encryption, but probably has not known it. Second, national security concerns have caused NSA to resist the spread of commercial and private encryption. NSA fears that strong, publicly available encryption will hinder its international intelligence gathering operations.

NSA has slowed the spread of encryption through its effective control of export licenses for encryption products.[4] While there are some exceptions, in general NSA refuses to grant licenses for strong encryption. For example, NSA allows mass market software with encryption capabilities to be exported under a blanket license, but only if the key size is 40 bits or less. This is akin to allowing combination locks to be exported, but only if they have 20 or fewer possible combinations. It falls far short of the current Federal Data Encryption Standard (DES) which employs 56-bit keys. A 40-bit key can be searched 65,000 times faster than one that is 56-bits long.

Export controls limit domestic as well as foreign entities. Along with the shift to a global economy, communications are becoming increasingly international in nature. Just as few people would buy a new telephone that could only be used domestically, market acceptance is limited for secure communications services and products that can only be used for communicating within the United States. American manufacturers are also loath to build high security devices for the domestic market for fear of drawing attention to the poor security of the export version and to avoid duplicate marketing efforts. Foreign software and hardware manufacturers which operate from nations with less onerous export controls therefore have a competitive advantage not only in their home country, but also in the US market. The U.S. Government limits the export, but not the import, of cryptographic products.

---

[4] While export licenses are granted by the State Department, it is generally recognized that State defers to NSA's expertise in this area.

An unavoidable tradeoff must be faced: If the Clinton Administration continues the policies of the past by discouraging strong commercial and private encryption, it aids American intelligence agencies in an important task: reading international message traffic to glean information of value to the American Government. But that policy also allows foreign intelligence agencies to read that same traffic and glean information of value to foreign governments – much of it involving confidential information of American citizens and corporations. This tradeoff needs to be carefully examined by those proposing the NII because, as noted earlier, without strong encryption there are three possibilities which could prove extremely embarrassing to the Clinton Administration:

- creating a white elephant that no one will use;
- creating a disaster if an insecure NII is used; or
- foreign dominance by a competing, secure III (International Information Infrastructure).

A Primer on Telephone Surveillance for Human Rights Organizations

September 1993

David Banisar
Washington Office
Privacy International

The expansion of telecommunications services around the world has made the worldwide dissemination of news and information much easier. New telephone, facsimile and electronic mail services have created opportunities for human rights groups to improve organizing, and to promote human rights through exchanges of information and exposure of government abuses. However, these new technologies are also subject to electronic surveillance by these same governments and others. For this reason, human rights advocates should be aware of the dangers and measures that can be taken to limit surveillance.

The scope of this paper is limited to electronic surveillance of oral and electronic communications.[1] And of course, there are many other methods for spying on human rights organizations.

This paper also does not cover the many national laws and international conventions that may restrict electronic surveillance. Human rights organizations may want to contact Privacy International directly about these policies.

Most types of electronic communication can be intercepted without a high level of expertise or expensive equipment. Surveillance equipment is not difficult to construct and is available in many electronics stores. Most manufacturers sell surveillance devices to any buyer, without restrictions. Thus, groups should be aware that both governments and private organizations can have the capability to electronically eavesdrop.

This does not mean that everyone should believe that they are always under surveillance. It is not practical for any government or group to wiretap all telephones and listen to every conversations simultaneously. Wiretapping is a labor intensive operation and requires considerable resources to conduct the taps and listen to the conversations. New technologies, such as computerized voice recognition, have not reached the level of sophistication and low cost to allow police forces to automatically eavesdrop on conversations.

Nonetheless, human rights groups should be concerned about the possibility of electronic eavesdropping. Human rights groups are likely targets of many types of surveillance. In 1991, wiretaps and microphones were found in the offices of the Mexican Human Rights Commission.[2] In 1993, officials discovered an office operated by the Guatemalan army in the Mail and Telegraphy Administration that intercepted mail sent to human rights advocates and labor organizers.[3] In the US, the Federal Bureau of Investigation in the 1980s monitored the activities of CISPIS, a group critical of US government policy in El Salvador. Litigation conducted by the Computer Professionals for Social Responsibility under the Freedom of Information Act also revealed that the FBI monitored computer networks used by political and advocacy groups.

---

[1] There are numerous other means of electronic surveillance including using miniaturized microphones and long distance eavesdropping from powerful microphones miniature and long distance video and infrared cameras. dataveillance-the use of computers to track transactional data such as purchases and monitoring of telephone subscriber information (pen registers metering, trap and trace devices) among others For an overview of these technologies, see M.L. Shannon. *Don't Bug Me The Latest High Tech Spy Methods* Paladin Press(1992)

[2] *See Facts on File*, Latin American and Caribbean News (May 2, 1991).

[3] United Press International, Officials Discover Office That Opened Guatemalan Mail (March 27 1993), UPI Guatemalan Post Office Scandal Widens (March 30, 1993)

Thus, there is an obvious need for human rights groups to be concerned with wiretapping: Governments often monitor human rights groups to discover what they know, who their sources are, and what their future activities will be. The lack of secure communications creates the threat of physical harm to many people in the human rights field.

Telephones

Wiretapping is the surreptitious interception of telephone conversations by a third person who is not a party to the conversation. In many countries, it is illegal. However, many forms of electronic eavesdropping are often difficult to detect. There are many locations in a telephone system where a wiretap can be placed. For example, microphones in the telephone's handset can be replaced with one that can also record or transmit to a remote receiver. Intercepts can also be placed at the telephone boxes in the basements of buildings, on the lines outside the house, or on the telephone pole junction box near the target. A common technique used by governments is to remotely monitor calls by having lines run from a telephone company central office where the local switching equipment is located to a monitoring station in a government office. Many of these techniques are undetectable to the target, especially in new systems, where the switching is electronic.[4]

Nearly all governments in the world conduct wiretaps. The United States arguably has the strictest controls on wiretapping in the world. In the US, a law requires a judicial warrant for domestic law enforcement wiretaps but a different law with less strict safeguards permits electronic surveillance for national security reasons. In the United Kingdom and France, the law allows the government to conduct extensive legal wiretaps for non-criminal investigation purposes. For example, it was disclosed in 1993 that French counter-intelligence agents wiretapped the telephones of prominent journalists and opposition party leaders during the mid-1980s. In the UK, several cases exposed the British government role in monitoring social activists groups.[5] Similar problems exist in other countries. The US Department of State, in its *Country Reports on Human Rights Practices for 1992*, reports widespread use of wiretaps by both government and private groups in dozens of countries.[6] In some countries, such as Honduras and Paraguay, the state owned telecommunications companies were active participants in helping the security services monitor human rights advocates.

There is a practical limit to the number of wiretaps that can be conducted at any one time. Because it is necessary to have a human listen to the conversation, labor and equipment costs create practical limits to surveillance. There are also technical difficulties in providing for a large number of taps. Recently, former members of the Soviet KGB disclosed that they could not tap everyone. They had the capability of wiretapping only 1,000 phone lines in Moscow and another 1,500 for the rest of Russia. [7] It was also recently disclosed that the East Germany police employed 10,000 people to

---

[1] See *Electronic Spying*. Mentor Publications (1976)

[5] For a survey of UK Wiretapping see Patrick Fitzgerald and Mark Leopold. *Stranger on the Line The Secret History of Phone Tapping*. Bodley Head (1987)

[6] United States Department of State *Country Reports on Human Rights Practices for 1992* (1993)

[7] *See* Rafayenko and Rubnikovich. "Total Eavesdropping Impossible." *Russian Press Digest* (April 8 1993)(from *Nezavisimaya Gazeta*)

conduct wiretaps and listen to conversations.[8]

Given this, it is not likely that every telephone can be monitored in a particular city but it is possible that the public phones nearest to the offices of human rights organizations are monitored. In France, counter-intelligence officers illegally wiretapped not only the telephones of journalists but also the bars and restaurants that they frequented.[9]

There are reports that well financed agencies, such as the United States National Security Agency, with its estimated budget of $US 10 billion per year, and UK's MI6 and GCHQ a developing sophisticated voice recognition systems that can be used to search international phone lines for key words in different languages. Those conversations found to have these words are automatically recorded.[10] It appears that this technology has not been widely disseminated beyond those agencies. Otherwise, police agencies in the United States such as the FBI would use it and that information would have to be disclosed in court hearings. Since the FBI does not appear to use this equipment, it is even less likely that any other countries' police forces, who have much smaller budgets, are using this technology. Thus, surveillance is generally limited to those wiretaps installed manually and listened to by human agents.

Cordless Telephones

Cordless telephones communications are especially easy to intercept. Many of the older models broadcast just at the top range of the AM radio band and conversations can be easily overheard with any AM radio. Newer models operate in the 49 MHz range and can be intercepted with an inexpensive radio scanner purchased at most electronics stores for under $US 100.00. The range of interception can extend to nearly one mile.

Several manufacturers now offer "privacy secure" cordless phones but these merely use a simple fifty year old technique known as "frequency shifting" that inverts the sound waves to limit eavesdropping. This system provides minimal security at best and can even be understood by the human ear after some practice.

New digital-based cordless phones may provide a slightly greater level of protection from the common listener, but these devices lack any form of sophisticated scrambling that would protect eavesdropping by government agencies. In addition, it is likely that new scanners will soon be available commercially that will be able to listen in on these conversations.

Cellular Phones

The cellular phone uses similar technologies to the cordless phone. It also broadcasts over airwaves like a radio. Inexpensive scanners are also available to intercept conversations. Newer scanners may limit eavesdropping but kits are readily available from electronic stores and mail order companies to remove those protections.

New cellular phones use a digital system which will be more difficult to intercept and also provide for clearer conversations. It is also easier to secure these telephones from eavesdropping. However, intelligence agencies in the United States and other countries have attempted to restrict the use of this technology. In Australia, the federal government rejected the request of the law enforcement agencies and ordered the operator of a new digital cellular system to commence operation without the capability to intercept the over the air portion of the conversation.[11]

---

[8] Comments of Hansjorg Geiger. German Federal Commission for the Stasi Files (April 14. 1993)

[9] David Banisar. "French Wiretapping Scandal Leads to Electoral Defeat." *13 The Privacy Times 3* (April 1. 1993).

[10] See James Bamford. *The Puzzle Palace*. Houghton Mifflin (1982)

[11] Bernard Lagan and Anne Davies. "New digital phones on line despite objections." *The Sydney Morning Herald* 28 April 1993

Secure Phones

There are methods to ensure that telephone conversations are not easily monitored. Secure phones, which use cryptography, a mathematical technique for scrambling conversations, are commercially available from many different companies including Motorola, TRW and AT&T. AT&T recently introduced an telephone attachment that connects to the handset cord and when used with a duplicate device on the receiving device, scrambles conversations. In the future, these AT&T devices will, however, implement a system known as the Clipper Chip, designed by the NSA. The keys to the system are held the US Government.[12] If other countries also begin using similar systems, it is likely that keys for users in that country will reside with their governments.

Other devices use the US Data Encryption Standard (DES) or company proprietary standards. DES is considered by most security experts to be secure. Secret propriety standards may not be as secure since they may have weaknesses that have not been publicly disclosed. There is also the possibility that the devices are deliberately not secure. The United State and some other countries have laws that prohibit the export of any device or software that contains unbreakable encryption without permission of the government. In the US, the NSA requires that manufacturers design their products that will be exported so that the NSA may still monitor the conversations. A method to circumvent these controls is to purchase secure devices from countries such as Sweden and Switzerland, which do not have export control laws on cryptography. However, these devices might have also been compromised by their domestic intelligence agencies. There are also international information sharing agreements such as the Quadripartite Agreement between intelligence agencies that may affect the security of the devices.[13]

It may also be illegal to use such devices. Some countries, such as France and Germany, prohibit the use of encryption without providing the keys to the government. These devices are also very expensive, ranging from $1-2,000 each.

Facsimile (fax)

It is also possible to intercept facsimile transmissions. A fax machine is essentially an inexpensive computer modem that uses a standard for sending and receiving files. Commercial devices are available that automatically intercept faxes. In 1992, it was reported that the U.S. Army purchased several $30,000 fax interception machines. Other are available for much less cost from manufacturers in the United States and elsewhere.

It is also possible to intercept faxes using tape recordings of transmissions. With the widespread use of Digital Audio Tape (DAT), it may become easier to record a fax transmission and with minimum effort to replay back into a machine. Thus, fax machines should be considered as insecure as telephones.

There are also fax machines available that provide scrambling to prevent interception. These machines usually cost around $US 2-3,000 and are available worldwide.[14] Like secure telephones, fax machines from the United States must have a weakened encryption scheme to allow for their export. Companies in Sweden, Switzerland, and other European countries claim their machines are not limited because they have no export laws. An expert on encryption should be consulted before

---

[12] White House Press Release on the "Clipper Chip" (April 16, 1993)

[13] *See* Simon Davies, *Big Brother*, Simon and Schuster (1992). Jeffrey Richelson, *The U S Intelligence Community* Harper (2nd ed 1989) Chapter 12

[14] For example TRW and Ricoh Canada sell the TRW Fax Encryptor 300 for $US 2,995 SecuriCrypto AB of Sweden sells the SecuriFax for $2 000

BOSTON PUBLIC LIBRARY
3 9999 05981 633 8

purchasing these devises to ensure their security.

Computer Communications

Electronic mail is one of the newest and most useful tools for human rights advocates. It provides fast and inexpensive communications to nearly every country in the world. It is also possible to create private mailing lists or public electronic conferences such as Peacenet or the USENET newsgroups such as Soc.Human.Rights where advocates can meet and exchange information and ideas.

Eavesdropping of computer communications is not difficult unless measures are taken to increase security. Currently, sending electronic mail is the equivalent of sending a typewritten postcard in the mail; it theoretically can be read by anyone between the author and the recipient and there is also no method to verify the identity of the originator of the message, thus it is possible to send forged messages out to disrupt the activities of a group. Some groups are already using encryption. It is reported that the African National Committee developed and used an encrypted e-mail network for years without it being compromised by the security services of South Africa.[15]

Encryption can be used to protect the messages and to verify the identity of the sending party. Unlike other communications technologies, encryption for computers is widely available for free or at minimal cost. It is also easy to use. Many commercial software packages such as Lotus Notes and the planned future versions of the Microsoft and Apple Computer operating systems will have built-in encryption, although the encryption in these products may have been weakened to allow for export. There are currently efforts to implement encryption as a standard for all electronic mail. Called Privacy Enhanced Mail (PEM), it will be several years before it will be available and in common use.

There is a program currently available at no cost that is ideal for international human rights advocates who use computers - Pretty Good Privacy (PGP). It was written by Phil Zimmermann, an American software engineer and privacy advocate who developed the program when it appeared that the US government was going to limit the use of encryption. PGP is available worldwide on many electronic bulletin boards and Internet sites. It is available for nearly every type of computer.[16] It also works in many different foreign languages. The program is small and can work on any laptop or personal computer. To use the program, a person writes out a message using a word processor, runs PGP to scramble it, then sends the scrambled file as a mail message. The receiver saves the message as a file and runs PGP to covert it back to a readable form. The process only takes an additional minute or two, depending on the length of the message and the processor speed of the computer. In some cases, programs have been written to make it an automatic function of electronic mail.

PGP uses "public key" encryption. Each user of PGP creates two keys, a public key and a secret key. The user then gives the public key to whomever they wish to correspond with. They can even publish it publicly like a phone number so long as they keep the secret key in a safe place (usually with the PGP program). The public key is used by other people to encrypt messages that they send to the user and only that user can unscramble the messages using the corresponding secret key. Thus, public key cryptography avoids the need to meet in person or through trusted messengers to distribute keys.

---

[15] Andrew Morris, Report from South Africa. International Privacy Bulletin, Volume 1, Issue 4 (October 1993).

[16] PGP is available for Atari, IBM PCs (and clones) & OS/2, Apple Macintosh, NeXT, Sun, VAX/VMS UNIX and IBM mainframes

Another feature that PGP and other public key systems can provide is "Digital Signatures," which ensure the identity of the sender of the message in the same way that a normal signature at the bottom of a letter usually verifies that a letter is from a known corespondent. Signatures are useful when an electronic message is sent to ensure that it was not modified or falsely created by someone else. Thus, readers of notices from groups which send out electronic alerts , such as Amnesty International, Americas Watch, Helsinki Watch and the Tibetan Government-in Exile, can ensure that the alerts have not been altered.

PGP can also be used to protect files on a computer. It can prevent the accessing of electronically stored papers or correspondence in case there is a physical break-in.

PGP 2.0 was developed in European countries without export controls so it is not required to limit its encryption strength. As of the writing of this paper, the latest version of PGP is 2.3a. A list of sites containing copies of the program can be obtained from the CPSR Internet Library via WAIS/Gopher/FTP to cpsr.org folder /cpsr/crypto. It can also be obtained by electronic mail. Send a message to listserv@cpsr.org with the word: help in the first line of text for information

Conclusion

New technologies offer new opportunities for human rights advocates. These same technologies also present opportunities for enhanced eavesdropping by those opposed to the NGO's activities.

Wiretapping of human rights groups is not an uncommon occurrence. However, there are limits, both technical and labor related to the number of taps that are in effect at one time. It is impracticable for every phone in a city to be monitored simultaneously. Nonetheless, human rights organizations may want to take precautions. There are methods available to prevent eavesdropping and care must be taken to ensure that the devices purchased actually provide an adequate level of protection.

Privacy International

Privacy International (PI) is an international human rights organization concerned with privacy, surveillance and data protection issues worldwide. It has members in over forty countries and is based in London, England with offices in Washington, DC and Sydney, Australia. PI also publishes a quarterly newsletter, the International Privacy Bulletin, that addresses worldwide updates on these issues.

More information on PI is available from the CPSR Internet Library in folder /privacy_international.

Yearly membership is $50 US for individuals, $200 for organizations.

For more information on PI and the International Privacy Bulletin, contact:

Privacy International
666 Pennsylvania Ave, SE, Suite 303
Washington, DC 20003 USA
Phone 1+(202)544-9240
Fax 1+(202)547-5482
Email: PI@washofc.cpsr.org

About the Author and Acknowledgments

David Banisar is a graduate of the Columbus School of Law, The Catholic University of America and the University of Maryland. Acknowledgments to Richard Claude, Simon Davies, Wayne Madsen, Marc Rotenberg, Dan Salcedo, and David L. Sobel.

ISBN 0-16-043370-3

90000

9 780160 433702